Lecture Notes

electronic health card

Michael Nüsken

b-it

(Bonn-Aachen International Center
for Information Technology)

summer 2008

To Do:

- a little number theory (math)
- a little cryptography (RSA, (HE), Signatures, Hash functions, PKI + certificates, ...)
- a little about smartcards, internet protocols (IPsec*, SSL/TLS)

finally: electronic health card and related infrastructure

Basics

~~ehc~~
ehc
9.04.08
2

* signature scheme: El Gamal

Setup: later.

Sign: later, derive this!

Verify: $g \in G = (G, \cdot)$ group, $a \in G$

Input: document x
signature $s = (b, \gamma)$

Output: Valid / Invalid.

1. Check

$$\boxed{a^{b^*} b^{\gamma} = g^{x}}$$

and answer Valid if it holds
and Invalid otherwise

Here G shall be a commutative group!

don't Proper: G is a set and $\cdot : G \times G \to G$ binary operation (well defined)

Associative: $\forall a,b,c: (ab)c = a(bc)$

Neutral: $\exists 1_G : \forall a: 1 \cdot a = a = a \cdot 1$

Inverses: $\forall a : \exists b : \quad a \cdot b = 1 = b \cdot a$

Commutative: $\forall a,b : \quad ab = ba$

Examples

$(\mathbb{Z}\setminus\{0\}, \cdot_{\mathbb{Z}})$ P ✓ A ✓ N ✓ ~~I~~ C ✓

not a group!

$(\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}, \cdot_{\mathbb{Z}})$, say $p = 5$.

~~I~~ not a group!

$(\mathbb{Z}_p, \text{"mod } p\text{"})$ $\quad a \cdot_{\text{mod } p} b = ?$

Tool: Division with remainder:

Given $n, d \in \mathbb{Z}$
there exist $q, r \in \mathbb{Z}$
such that
$$n = q\,d + r$$
and $0 \le r < d$

$n \text{ div } d := q \quad (\in \mathbb{Z}!)$

$n \text{ rem } d := r \quad (\in \mathbb{Z}!)$

Alternatively, use $n \text{ rem } d$ in our "domain" $\mathbb{Z}_d$:

$$\mathbb{Z} \longrightarrow \mathbb{Z}_d = \{0, 1, 2, \dots, d-1\}$$
$$n \longmapsto \text{"}n \text{ rem } d\text{"} = n \bmod d.$$

Example:

$4 \cdot 5 = 6$ in $\mathbb{Z}_7$

$(11 \cdot 5) \bmod 7 = 6$

$(18 \cdot (-2)) \bmod 7 = 6$

$$a \cdot_{\mathbb{Z}_p} b = (\tilde{a} \cdot_{\mathbb{Z}} \tilde{b}) \bmod p$$

ehc
9.4.08
4

$(\mathbb{Z}_p, \cdot_{\mathbb{Z}_p})$ P ✓ A! N ✓ ~~I~~ C ✓

0 has no inverse!

$\mathbb{Z}_p^\times := (\mathbb{Z}_p \setminus \{0\}, \cdot_{\mathbb{Z}_p})$, p prime!

P ✓(!) A ✓ N ✓ I! C ✓

(later!)

This is a group.
And it's the one we use for ElGamal signatures.

$(\mathbb{Z}, +)$ P ✓ A ✓ N: 0 ✓ I: − ✓ C ✓

$(\mathbb{Z}_p, +_{\mathbb{Z}_p})$ $a +_{\mathbb{Z}_p} b := (\tilde{a} +_{\mathbb{Z}} \tilde{b}) \bmod p$

P ✓ A ✓ N: 0 ✓ I: − ✓ C ✓

$(\mathbb{R} \setminus \{0\}, \cdot)$ PANIC ✓
$(\mathbb{R}, +)$ PANIC ✓

$\mathbb{R}$ is a field!

Note: we can never compute all digits of $3^{2^{160}} \in \mathbb{Z}$

But it's easy to compute

$3^{2^{160}}$ in $(\mathbb{Z}_{10^{100}+37}) \cdot \mathbb{Z}_{101}$.

Actually: $3^{(2^{160})} = 3$ in $\mathbb{Z}_{101}$.

ehc 3.4.08 5

How can I know?

How can we check?

Aposki's law $(a^b)^c = a^{(b\cdot c)}$

toy example:

How to compute 3^{12} in $\mathbb{Z}_{101}$? Nikoofar's law: $a^b a^c = a^{b+c}$

Start: 3^2, $(3^2)^2 = 3^4$, $(3^4)^2 = 3^8$

$$3^8 \cdot 3^4 = 3^{8+4} = 3^{12}.$$

Do it:

$9, -20, -4, 16$

$$-64 = 37 \text{ in } \mathbb{Z}_{101}. \qquad 3^{12}$$

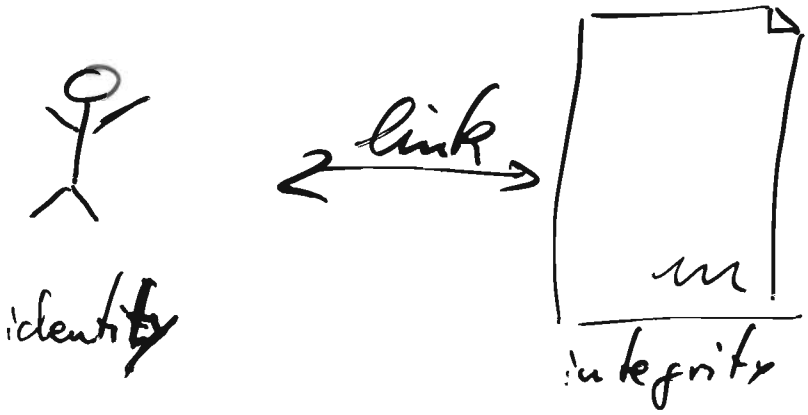
How many operations for $3^{(2^{160})}$ in $\mathbb{Z}_{101}$?

160 squarings ($\hat{=}$ multiplication) in $\mathbb{Z}_{101}$.

Inbetween: Karatsuba multiplication $O(n^{\log_2 3})$

One multiplication modulo an n-bit number takes $O(n^2)$ bit operations by using school method (for integer multiplication and integer division). Best known ~~$O(n \log n \log\log n)$~~ $O(n \log n \log\log n)$, maybe $O(n \log n \, 2^{\log^* n})$

Real life signature



Electronic signature does more or less the same.

When we consider an electronic signature scheme it will

(P) consist of a setup, a signing and a verification algorithm (or protocol) and possibly more.

(C) be correct, ie. after honest setup and signing the verification must always (or mostly) return 'Valid'.

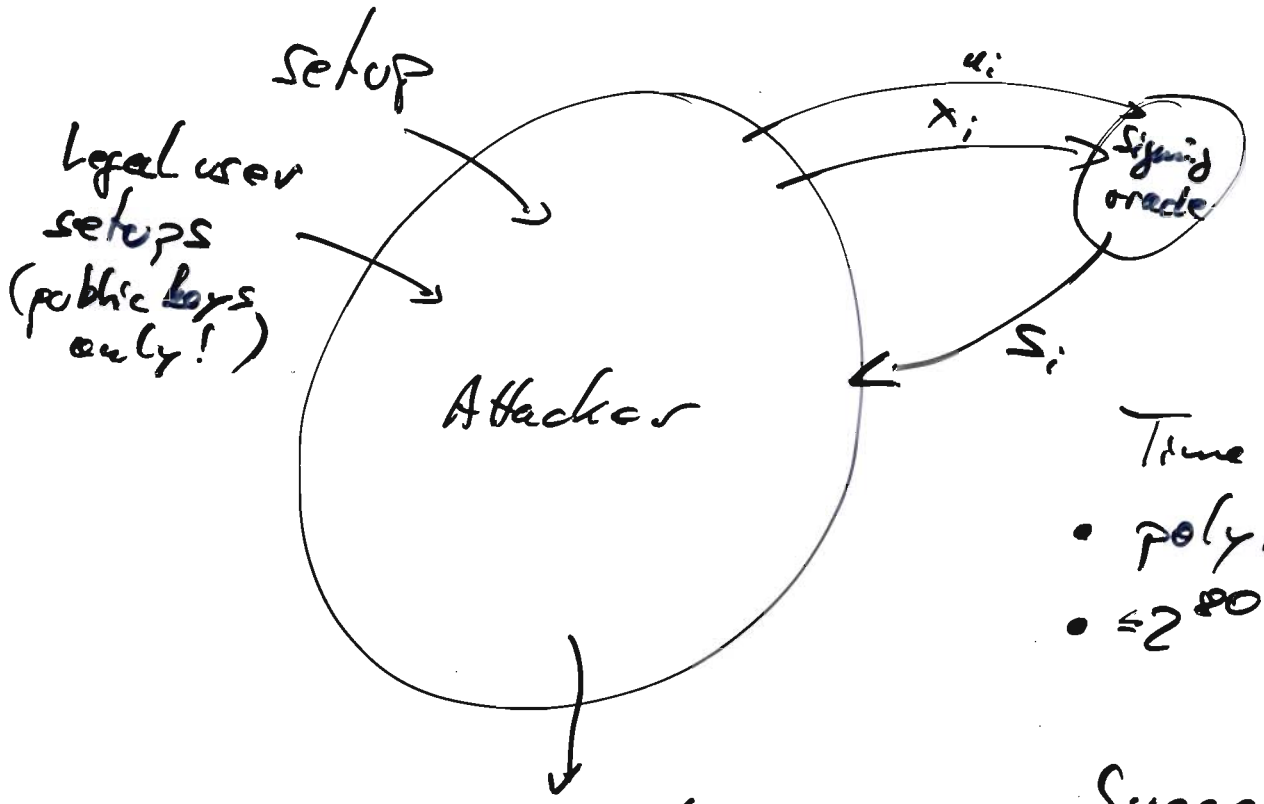
(E) be efficient, ie. time and space should be within reasonable bounds.

- so that benefit is larger than cost.
- fix size bound: 2^{40} op's, 2^{30} space.
- polynomial (asymptotic view).

(S) be secure, ie. ?

Security goal?

⚠ Protect against <u>any</u> reasonable attacker.



Time + Space:
- polytime
- $\leq 2^{80}$.

document x
+ ~~valid~~ signature s
for one legal user u

Success:
the signature s is accepted by the verification on document x for user u, and the doc x has not been queried to oracle for user u.

prob(Attacker succeeds)
$\geq$ prob(Guessing) + $\frac{1}{n^c}$
for large n, some c.

<u>SECURITY GOAL</u> There is no such attacker!

The ring of integers modulo N

ehc
16.4.08

(1)

N is any natural number, $N \geq 2$.

By abuse of notation

$\mathbb{Z}_N$ set $\{0, 1, 2, \dots, N-1\} =: \mathbb{Z}_N$

(alternatively: $\{-\lfloor \frac{N-1}{2} \rfloor, \dots, -1, 0, 1, \dots, \lfloor \frac{N-1}{2} \rfloor\}$)

This should be N elements... check it out...

$+_{\mathbb{Z}_N} : \mathbb{Z}_N \times \mathbb{Z}_N \longrightarrow \mathbb{Z}_N$ binary op.

$$a +_{\mathbb{Z}_N} b := (\tilde{a} +_{\mathbb{Z}} \tilde{b}) \bmod N.$$

Ex: $4 +_{\mathbb{Z}_7} 5 = 2$.

$\cdot_{\mathbb{Z}_N} : \mathbb{Z}_N \times \mathbb{Z}_N \longrightarrow \mathbb{Z}_N$ binary op.

$$a \cdot_{\mathbb{Z}_N} b := (\tilde{a} \cdot_{\mathbb{Z}} \tilde{b}) \bmod N.$$

Ex $4 \cdot_{\mathbb{Z}_7} 5 = 6$.

comm. Ring

P+ A+ N+ I+ C+

$\downarrow$ $\downarrow$

0 $-$

P· A· N· $\cancel{I}$· C·

$\downarrow$

1

$0 \neq 1$

D ON'T

$\downarrow$

$\forall a, b, c \in \mathbb{Z}_N$: $a(b+c) = ab + ac$,

$(a+b)c = ac + bc$

Ring = DON'T PANIC, PAN!

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

Example 2×2 matrices over $\mathbb{Z}_3$ form a ring: $\mathbb{Z}_3^{2 \times 2}$, here the mult is not comm.

We never have an inverse for 0.

Thm: $a0 = 0a = 0$ for any a in a ring.

~~N.: $1a = a = a \cdot 1$~~

~~Together: $0 = 0 \cdot 1 = 1$~~

Suppose $\exists a$: $\underset{\underset{0}{\parallel}}{a \cdot 0} = 1$ ← Thm. but that contradicts $0 \neq 1$.

ehc 16.4.08 (2)

But what about the rest? $\mathbb{Z}_N \setminus \{0\}$?

1 always has an inverse: $1 \cdot 1 = 1$.

Say we are given $x \in \mathbb{Z}_N$ and want to find y such that $y \cdot x = 1$ in $\mathbb{Z}_N$.

By definition that means that

$$\tilde{y} \cdot_{\mathbb{Z}} \tilde{x} + t \cdot N = 1 \quad \text{in } \mathbb{Z}$$

for some $t \in \mathbb{Z}$. Actually we want to solve

$$\underbrace{s\,\tilde{x} + t\,N} = 1 \quad \text{in } \mathbb{Z}$$

for $s, t \in \mathbb{Z}$.

Instead of directly solving, let's try to find s, t such that

$$s\,\tilde{x} + t\,N$$

is "small": absolute value small but non-zero.

Example $N = 17, \quad \tilde{x} = 7.$

s	t	$s \cdot 7 + t \cdot 17$	
-1	1	10	
0	1	17	$= 0 \cdot 7 + 1 \cdot 17$
1	0	7	$= 1 \cdot 7 + 0 \cdot 17$
		10	$= (-1) \cdot 7 + 1 \cdot 17$

$| - 1$

---

r	q	s	t	comment
17		1	0	$17 = 1 \cdot 17 + 0 \cdot 7$
7	2^*	0	1	$7 = 0 \cdot 17 + 1 \cdot 7$
3	2	1	-2	$3 = 1 \cdot 17 + (-2) \cdot 7$
1	3	-2	5	$1 = (-2) \cdot 17 + 5 \cdot 7$
0		7	-17	$0 = 7 \cdot 17 + (-17) \cdot 7 \quad 17 \overset{*}{=} 2 \cdot 7 + 3.$

This is called the Extended Euclidean Algorithm (EEA).

Thus: the last line tells us

$$0 = 7 \cdot 17 + (-17) \cdot 7$$

so it gives us a cross check.

the one but last line tells us

$$1 = (-2) \cdot 17 + 5 \cdot 7$$

and so (applying mod 17): $1 = 5 \cdot_{\mathbb{Z}_{17}} 7$, i.e. $7^{-1} = 5$.

Example 2

$21 \in \mathbb{Z}_{36}$. What'd be the inverse if any?

We look for

$$t \cdot 21 + s \cdot 36 = 1 \quad \text{in } \mathbb{Z}$$

i	r	q	s	t
0	36		1	0
1	21	1	0	1
2	15	1	1	-1
	6	2	-1	2
	3	2	3	-5
	0		-7	12

$$36 = \underset{q_1}{1} \cdot 21 + \underset{r_2}{15}$$

Div. with remainder

$$21 = 1 \cdot 15 + 6$$
$$= 2 \cdot 15 - 9$$
$$15 = 2 \cdot 6 + 3$$

Cross-check: $0 = \underset{-21/3}{(-7)} \cdot 36 + \underset{36/3}{12} \cdot 21$

The one-but-last line tells us:

$$3 = 3 \cdot 36 + (-5) \cdot 21.$$

and ... 3 divides both 36 and 21

and thus also $t \cdot 21 + s \cdot 36$

but $3 \nmid 1$, thus we cannot have a solution and no inverse.

Notation: $a \mid b \;:\Leftrightarrow\; \exists c : \; a \cdot c = b.$

$a \nmid b \;:\Leftrightarrow\; \neg (a \mid b)$

Theorem

The EEA computes the greatest common divisor g of two given integers a, b and the representation

$$g = s \cdot a + t \cdot b.$$

It always terminates.
It uses at most $\mathcal{O}(\max(|a|, |b|))$ rows.
It uses at most $(2 \log_2 \max(|a|, |b|))$ rows.

[Actually, $|r_{i+2}| \leq \frac{1}{2} |r_i|$. ...]

Corollary

If the EEA for $\tilde{x}$ and N outputs $g = s\,\tilde{x} + t\,N$, $g, s, t \in \mathbb{Z}$.

then if $g = 1$ the element $\overset{\tilde{x} \bmod N}{x} \in \mathbb{Z}_N$ is invertible with inverse $s \bmod N \in \mathbb{Z}_N$.

and if $g \neq \pm 1$ (ie. $g \neq 1$) the element $x \in \mathbb{Z}_N$ <u>has no</u> inverse.

Pf Case $g = 1$ ✓

Case $g \neq \pm 1$: Then $g \mid \tilde{x}$ and $g \mid N$ thus $g \mid \bar{s}\tilde{x} + \bar{t}N$ but $g \neq 1$. □

<u>Corollary</u>

The set $\mathbb{Z}_N^\times$ of invertible elements is precisely

$$\{ \hat{x} \bmod N \in \mathbb{Z}_N \mid \gcd(\hat{x}, N) = 1 \}$$

and moreover it forms a group with multiplication.

<u>Def</u> $\mathbb{Z}_N^\times = (\mathbb{Z}_N^\times, \cdot)$

the set of invertible elements.

is the <u>unit group</u> of the ring $\mathbb{Z}_N$.

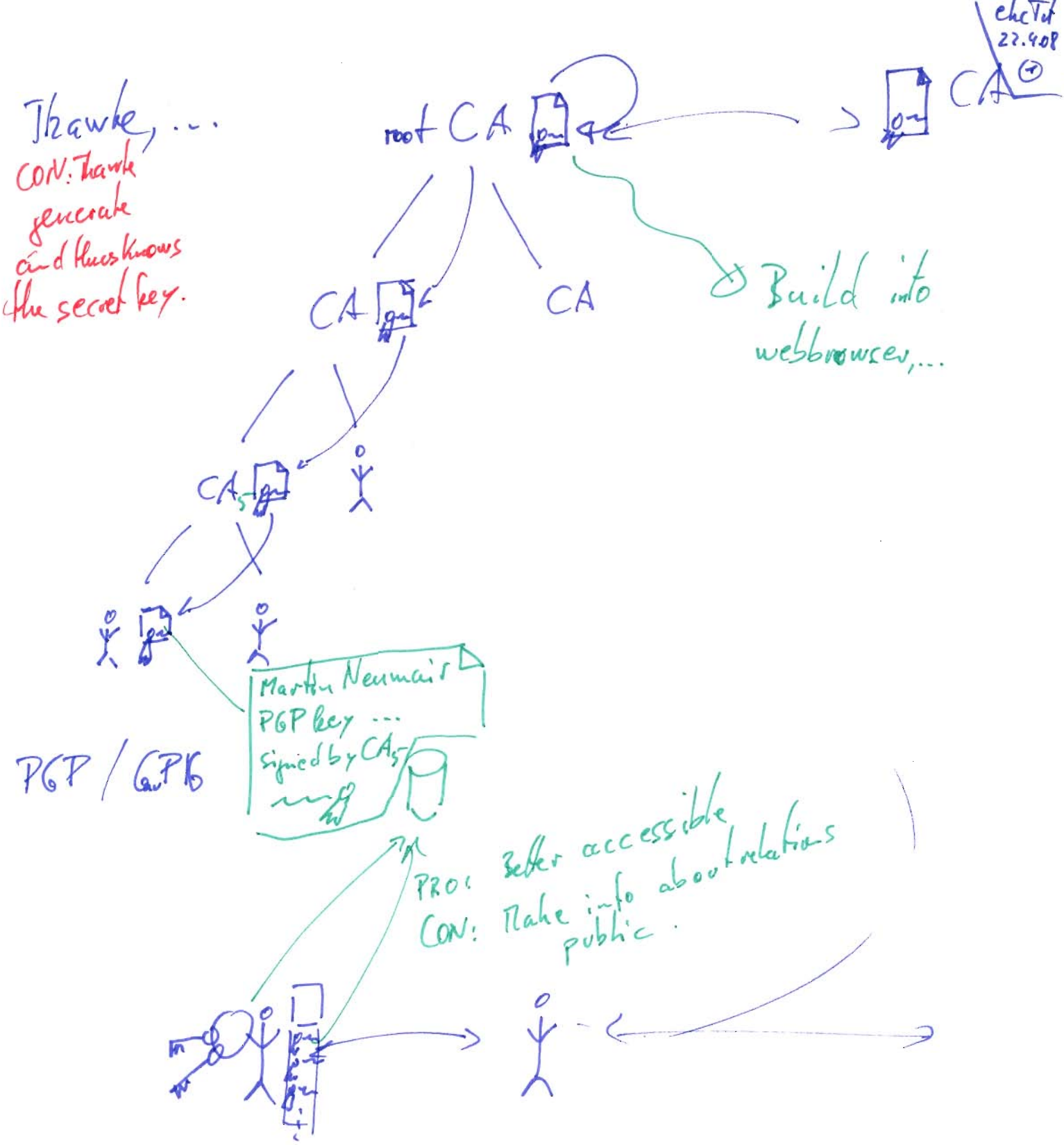
[Similarly: $\mathbb{Z}^\times = (\{\pm 1\}, \cdot_{\mathbb{Z}})$,

$\mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot_{\mathbb{R}})$.]

How to compute a power?

<u>Thm</u> Using square and multiply to compute a power.

We need at most $\Theta(\log_2 |e|)$ multiplications to compute g^e in $\mathbb{Z}_N$.


Thawte, ...
CON: Thawte generate and thus knows the secret key.
root CA
CA
CA
CA
Build into webbrowser, ...
CA5
Martin Neumair
PGP key ...
signed by CA5
PGP / GPG
PRO: Better accessible
CON: Make info about relations public.

ehc
22.4.08
2

EEA i	r_i	q_i	s_i	t_i
0	91		1	0
1	39	2	0	1
2	13	3	1	$\boxed{-2}$
3	0		-3	7

$91 = \underline{2} \cdot 39 + 13$

$39 = 3 \cdot 13 + 0$

X check: $\underset{-39/13}{-3} \cdot 91 + \underset{91/13}{7} \cdot 39 = 0$

Bézout equality

ad: $\boxed{\underline{13} = \underline{1} \cdot 91 + \underline{(-2)} \cdot 39}$ is the gcd of 91, 39.

So what about the inverse of $39 \in \mathbb{Z}_{91}$.

There is none. $\ulcorner$ $t \cdot 39 = 1$ in $\mathbb{Z}_{91}$.

ie. $s \cdot 91 + t \cdot 39 = 1$ in $\mathbb{Z}$.

but $13 \mid (s \cdot 91 + t \cdot 39)$

but $13 \nmid 1$. $\lrcorner$

i				
0	91		1	0
1	17	5	0	1
2	6	3	1	-5
3	-1	-6	-3	16
4	0		-17	91

$91 = \overset{b}{5} \cdot 17 + 6$

$17 = 3 \cdot 6 - 1$

$6 = (-6) \cdot (-1) + 0$

Xcheck! $0 = -17 \cdot 91 + 91 \cdot 17$ ✓

gcd: $-1 = -3 \cdot 91 + (+16) \cdot 17$

Division with remainder

$$\boxed{a, b \neq 0 \to \exists q, r : \quad a = q \cdot b + r \quad \& \quad 0 \leq r < |b|}$$

Def

$$\boxed{g \in \gcd(a,b)} \iff g \mid a \wedge g \mid b \wedge \forall d \, (d \mid a \wedge d \mid b \Rightarrow d \overset{\leq}{\mid} g)$$

Lemma $g, \hat{g} \in \gcd(a,b)$ Then $g \mid \hat{g}$ and $\hat{g} \mid g$.

ie. $gu = \hat{g}$ and $\hat{g}v = g$

for some u, v.

Then $guv = \hat{g}v = g$

thus* $uv = 1$, ie. u, v are invertible

*in rings with cancellation property (integral domain)

Conclusion: Two gcd's are always equal up to a unit (invertible element).

Doing without division with remainder:

$\mathbb{Z}[X]$.

Try $a = 1 \cdot X + 1$, $b = 2X$.

then $a = q \cdot b + r$

has ~~the~~ only solutions with $\deg(r) \geq 1$.

But when you consider univariate polynomials over a field then you do have division with remainder:

$\mathbb{Q}[X]$.

$$(X+1) = \underbrace{\tfrac{1}{2}}_{q} \cdot (2X) + \underbrace{1}_{r}.$$

$$1 \cdot X + 1 = \left(\tfrac{1}{2}\right) 2X + 1.$$

divide by this!
In a field you can always do that

$\frac{1}{2} \cdot 2X = X$

$\boxed{0} X + 1$

We use: $\mathbb{F}_2[X]$!

$\mathbb{F}_2$ is <u>the</u> field with 2 elements: $\mathbb{Z}_2$

$$\mathbb{F}_2 = \mathbb{Z}_2 \cong (\{F, T\}, \overset{\oplus}{\vee}, \wedge) \cong (\{\text{🌸}, \text{🍎}\}, \square, \diamond)$$

How to define division with remainder in a univariate polynomial ring?

Thm: Given $a, b \in F[X]$, $b \neq 0$.
F ← a field.

THEN: There exists $q, r \in F[X]$ such that

$$a = q \cdot b + r$$

and

$$\deg(r) < \deg(b)$$

[side remark: $\deg(0) := -\infty$.]

Using this we run the EEA on

$$1 + x + x^3 + x^4 + x^8 \in \mathbb{F}_2[x],$$
$$1 + x + x^3 \in \mathbb{F}_2[x].$$

Bézout coefficients

r	q	s	t
$a = 1+x+x^3+x^4+x^8$	–	1	0
$1+x+x^3$	$1+x^2+x^3+x^5$	0	1
x^2	x	1	$1+x^2+x^3+x^5$
$1+x$	$1+x$	x	$1+x+x^3+x^4+x^6$ $x+x^2+x^4+x^5+x^7$
1	$1+x$	$1+x+x^2$ $x+x^2+x^3$	x^6+x^7 x^7+x^8
0		$1+x+x^3$	$1+x+x^3+x^4+x^8$

✗ check ✓

$$1+x+x^3+x^4+x^8 = (1+x^2+x^3+x^5)(1+x+x^3) + x^2$$

$$\begin{array}{r|l} x^8+x^4+x^3+x^2+x & x^5+x^3+x^2+x \\ x^8+x^7+x^6+x^5+x^3 & x^3+x^2+x \\ \hline x^7+x^6+x^5+x^4+x^2+x & x^2+x \\ x^7+x^6+x^5+x^4+x^3+x^2 & x^2+x \\ \hline x^3+x & x^2+x \\ x^3+x^2+x & x^2+x \\ \hline x^2 & x^2+x \end{array}$$

Thus: $1 = (1+x+x^2)\cdot a + (x^6+x^7)\cdot(1+x+x^3)$.

ie the inverse of

$$1+x+x^3 \in \underbrace{\mathbb{F}_2[X] / \langle \underbrace{1+x+x^3+x^4+x^8}_{=:a} \rangle}_{} =: R$$

is x^6+x^7.

This is another ring!

Actually, a is irreducible,

ie. there is no non-trivial factorization:

$$\boxed{a = d_1 \cdot d_2 \Rightarrow d_1 \mid 1 \vee d_2 \mid 1}$$

Thus R is a field!

with $2^8 = 256$ elements.

~~2^8-1 not trivial~~

Remember: $\mathbb{Z}_{256}$ is <u>not</u> a field.

Actually <u>Thm</u> For every prime power $q = p^e$, p prime, $e \in \mathbb{N}_{>0}$ there exists essentially one field $\mathbb{F}_q$ with q elements. For non-prime powers N there is no field with N elements.

$x^4 + x^2 + 1 \in \mathbb{F}_2[X]$ irr? No $:= (x^2+x+1)^2$.

$x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[X]$ irr? No.

$\shortparallel$

$(x-1) \cdot q + r$

$r = 0$ ← since $|_{x=1}$ we get zero in $x^4+x^3+x^2+1$.

$x^4 + x^3 + 1 \in \mathbb{F}_2[X]$ is irr!

$x^4 + x + 1 |_{x = 1/y} \cdot y^4$

$x^4 + x^3 + x^2 + x + 1$ is irr!

$$\rightarrow \quad \mathbb{F}_2[X] / \langle x^4 + x + 1 \rangle \cong \mathbb{F}_{2^4}.$$

$$\cong$$

$$\mathbb{F}_2[y] / \langle y^4 + y^3 + 1 \rangle$$

$$\cong$$

$$\mathbb{F}_2[z] / \langle z^4 + z^3 + z^2 + z + 1 \rangle$$

Outlook:

- EEA proofs.
- Groups: Thms Lagrange, Euler, Fermat

$x^{\#G} = 1$

Applied to $\mathbb{F}_q$ gives: $x^q = x$ for all $x \in \mathbb{F}_q$.

i.e. $\underline{x^q - x} = 0 \Rightarrow$ ↯!

ehc
23.4.08
1

i	r_i	q_i	s_i	t_i
17	r_{17}		s_{17}	t_{17}
18	r_{18}	q_{18}	s_{18}	t_{18}
	r_{19}		s_{19}	t_{19}

$$r_{17} = \underline{q_{18}} \cdot r_{18} + \underline{r_{19}}$$

$$0 \le r_{19} < |r_{18}| \quad (*)$$

"r_{19} smaller than r_{18}"

Given. $r_{i-1}, s_{i-1}, t_{i-1}$

$r_i \quad s_i \quad t_i$

Do this:

$$\left.\begin{aligned} q_i &= r_{i-1} \text{ div } r_i \\ r_{i+1} &:= r_{i-1} - q_i r_i \end{aligned}\right\}$$

STOP if $r_{i+1} = 0$

$$s_{i+1} := s_{i-1} - q_i s_i$$

$$t_{i+1} := t_{i-1} - q_i t_i$$

$r_0 = a \qquad s_0 = 1 \qquad t_0 = 0$

$r_1 = b \qquad s_1 = 0 \qquad t_1 = 1.$

<u>Ex 2.3 (iv)</u> Claim: $r_i = s_i a + t_i b. \quad (i \ge 0)$

<u>Pf</u> $i=0$: $a = r_0 \overset{?}{=} \underset{1}{\underset{\shortparallel}{s_0}} a + \underset{0}{\underset{\shortparallel}{t_0}} b = a.$ ✓

$i=1$: ... ✓

$i+1>1$: By hypothesis: $r_{i-1} = s_{i-1} a + t_{i-1} b$

$r_i = s_i a + t_i b \quad | \cdot(-q_i)$

Thus: $r_{i+1} \overset{\checkmark}{=} s_{i+1} a + t_{i+1} b$ $\square$

Ex 2.3 (v) $\forall i \geq 1$: $\underbrace{\gcd(r_i, r_{i+1})}_{g} = \underbrace{\gcd(r_{i-1}, r_i)}_{h}$

ehc 23.4.08 (2)

Pf we have: $\boxed{r_{i+1} = r_{i-1} - q_i r_i}$.

Note: • $g \mid r_i \wedge g \mid r_{i+1}$.

•• $\forall d \; (d \mid r_{i-1} \wedge d \mid r_i \Rightarrow d \mid h)$

Does $g \mid r_{i-1}$?

Remember: $\boxed{r_{i-1} = \underbrace{r_{i+1}}_{c_{i+1} g} + \underbrace{q_i r_i}_{q_i \cdot c_i g}}$.

$(c_{i+1} + q_i c_i)\, g$

that is: $g \mid r_{i-1}$!

Thus by •• $g \mid h$.

Similarly $h \mid g$.

$g \simeq h$ (equal up to unit!). $\square$

i.e. $g = uh$ for some invertible element u

Let ℓ be the index last non-zero remainder, i.e. $r_\ell \neq 0$, $r_{\ell+1} = 0$.

Ex 2.3 (vi)

$$\gcd(r_e, 0) = r_e$$

Pf Clearly: $r_e \mid r_e \wedge r_e \mid 0$.

Now consider $d \mid r_e$, $d \mid 0$.

So $d \mid r_e$. $\square$

Ex 2.3 (~~vi~~ a)

EEA is correct provided it terminates,

i.e. $g = \gcd(a, b)$

and $g = s_e \cdot a + t_e \cdot b$

with $g := r_e$.

Pf. Induction: $\gcd(a,b) \overset{(v)}{=} \gcd(r_{i+1}, r_{i+1})$ ✓

$= \gcd(r_e, 0)$

$\overset{(vi)}{=} r_e = g$. ✓

By (iv) $r_e = s_e a + t_e b$. ✓ $\square$

Moreover: $0 = s_{e+1} a + t_{e+1} b$ as a X check!

Ex 2.3 (vii) $i \geq 1$: $|r_{i+1}| < |r_i|$ Obvious. ✓

Assume we never reach zero.

Then $0 < |r_j| < |r_{j-1}| < |r_{j-2}| < \dots < |r_1|$

$+1 \quad +1 \quad +1$

Thus $j \leq |r_1|$ for all j. ↯ $\square$

Ex 2.3 (viii)

ehc
23.4.08
(4)

$\forall\, i \geq 2, i \leq \ell$: $\quad |r_{i+1}| < \frac{1}{2}\, |r_{i-1}|$

Pf By def: $\quad r_{i+1} = r_{i-1} - q_i r_i$

$|r_{i+1}| < |r_i|$.

Consider cases: $\quad |r_i| \leq \frac{1}{2}|r_{i-1}|$

or $\quad |r_i| > \frac{1}{2}|r_{i-1}|$ $\square$

Thus $\ell \leq \underbrace{2 \log_2 \max(|r_1|, |r_0|)}_{O(n)}$.

so $\quad 1 \leq |r_\ell| < \frac{1}{2}|r_{\ell-2}| < \frac{1}{2^2}|r_{\ell-4}|$

$$\cdots < \begin{cases} \frac{1}{2^{\ell/2}} & |r_0| \\ \frac{1}{2^{\frac{\ell-1}{2}}} & |r_1| \end{cases}$$

ie. $\quad \ell \in O(n)$

and so $\quad$ runtime $\in O(n^3)$. $\square$

Actually: $\quad$ runtime $\in O(n^2)$

Further: if $g > 1$ then $g \mid a$ and $g \mid b$

thus $g \mid sa + tb$ for any s, t.

thus $g \mid 1$ if there would be a solution to $1 = sa + tb$ for $g > 1$. $\square$

Side remark:

Multiplication of n-bit integers

needs

$O(n^2)$ op-s with school method

$O(n^{\log_2 3})$ op-s with Karatsuba

$\log_2 3 \approx 1.57?$

$$(a_1 g + a_0) \cdot (b_1 g + b_0)$$

$$= a_1 \cdot b_1 \, g^2 + (a_1 \cdot b_0 + a_0 \cdot b_1) g + a_0 \cdot b_0 .$$

ie. 1 full size multiplication
= 4 half size multiplications.

but:

$$c_2 = a_1 \cdot b_1$$

$$c_0 = a_0 \cdot b_0$$

$$c_1' = (a_1 + a_0) \cdot (b_1 + b_0)$$

ie. $c_1' = \underbrace{a_1 b_1} + \underbrace{a_1 b_0 + a_0 b_1} + \underbrace{a_0 b_0}$

$$c_1 = c_1' - c_2 - c_0 .$$

ie. 1 full-size mult
= 3 half size mult. !

$\rightarrow O(n^{\log_2 3})$

Even better:

Schönhage – Strasse (1971)

$O(n \log n \log\log n)$ FFT.

only better than prior for $n > 1000(0)$?

Fürer (2007)

$O(n \log n \; 2^{\log^* n})$

$\log^* n = \min\{k \mid n \le \underbrace{2^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}}_{k}\}$

for our universe $\log^* n \le 5$.

$\underset{1}{2=2}, \; \underset{2}{2^2=4}, \; \underset{3}{2^4=16}, \; \underset{4}{2^{16}=65536}, \; \underset{5}{2^{65536}}$,

$n = \#\text{bits} \rightarrow$ ie. the number $N \approx 2^n = 2^{(2^{65536})}$

Realistic mem. bounds: 10^{30} bytes.

$kB = 10^3 = 2^{10}$ $\quad 2^{50}$

$MB = 10^6 = 2^{20}$ $\quad 2^{60}$

$GB = 10^9 = 2^{30}$

$TB = 10^{12} = 2^{40}$

Remember:

To compute the inverse of $a \in \mathbb{Z}_N$ decide and run the EEA on N, a.

From the result $g = sN + ta$

check $g = 1$ $(g \mid 1)$. then $a^{-1} = t$ in $\mathbb{Z}_N$

otherwise there exists no inverse.

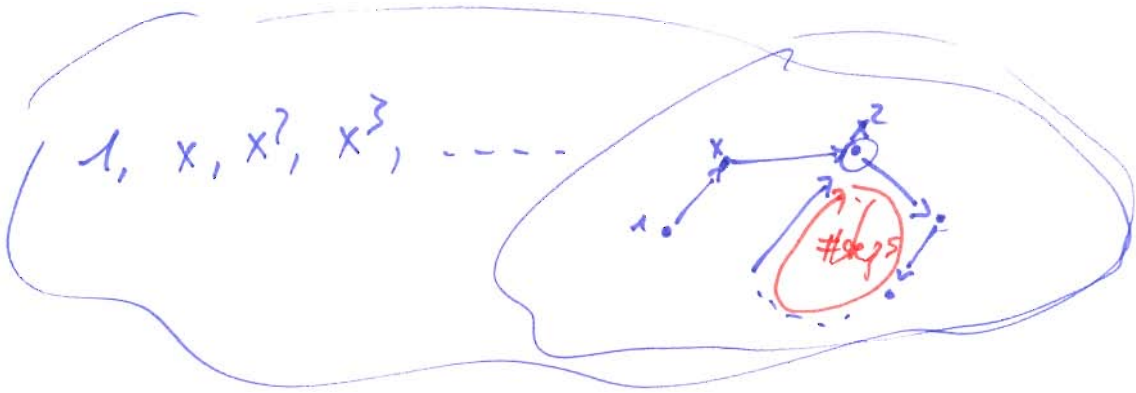
We also had:

- $\mathbb{Z}_N^\times$ unit group of $\mathbb{Z}_N$.

And $\mathbb{Z}_N$ is a field iff $\mathbb{Z}_N^\times = \mathbb{Z}_N \setminus \{0\}$.

Next topic:

Groups, Thm Lagrange, Euler, Fermat.



Groups

G is a group, commutative
ie. $\underset{\downarrow}{PANI(C)}$.
$G = (G, \cdot)$

Examples
- $\mathbb{Z}_N^\times$, R ring. Then $R^\times$ is a group.
- $GL_2(\mathbb{F}_q) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_q^{2\times 2} \mid \underset{\substack{\parallel \\ ad-bc}}{\det\begin{pmatrix} a & b \\ c & d \end{pmatrix}} \neq 0 \}$

  is a group, non-commutative.

Let's only consider finite groups, ie. $\#G \in \mathbb{N}$.
Consider an element $x \in G$ and look at the sequence:

$$1, \ x, \ x^2, \ x^3, \ \ldots$$

Thus since G is finite there must exist $i < j \in \mathbb{N}$ such that

$$x^i = x^j.$$

Then

$$1 = x^{j-i}.$$

(just divide by x^i).

Q: Which ~~possi~~ exponents e give us $x^e = 1$?

Of course: $x^0 = 1$.
Further: there must exist $0 < e \leq \#G$: $x^e = 1$.

etc
29.4.08
(2)

Put in structure.

<u>Ex</u>: $\mathbb{Z}_9^\times$, ~~MAN~~. Recall $\# \mathbb{Z}_9^\times = 6$.

$x=4$ gives $1, 4, -2, 1, 4, -2, 1, 4, -2, \ldots$

so we observe: it repeats every 3 steps.

$x=2$ gives $1, 2, 4, -1, -2, -4, 1$

so we observe: it repeats every 6 steps.

$x=-1$ gives $1, -1, 1,$ it repeats every 2 steps.

$x=-4 \longrightarrow$ repeats every 6 steps.

Actually, $x=2$ or $x=-4$ give us all elements of $\mathbb{Z}_9^\times$.

<u>Ex</u> $\mathbb{Z}_{10}^\times$. $\# \mathbb{Z}_{10}^\times = \#\{\pm 1, \pm 3\} = \boxed{4}$.

$x = 1 \longrightarrow$ repeats $\boxed{1}$.

$x = -1 \longrightarrow$ $\boxed{2}$.

$x = 3$: $1, 3, -1, -3$ repeats every $\boxed{4}$ steps.

$x = -3$ $\boxed{4}$ steps.

<u>Ex</u> $\mathbb{Z}_{40}^\times$. $\# \mathbb{Z}_{40}^\times = 2^2 \cdot 4 = \boxed{16}$. $40 = 2^3 \cdot 5$

$x = 3$: $1, 3, 9, 27 = -13, 1$ repeats every $\boxed{4}$ steps.

<u>Observation</u>: $\#\text{steps} \mid \#G$

Consequently: $x^{\#G} = 1$.

ehc
29.4.08
3

Thm (Lagrange)

Given a finite commutative group G and an element $x \in G$.

Then
$$x^{\#G} = 1 .$$

Pf (commutative)

Form a list of all elements in G, $d = \#G$:

$$x_0, x_1, x_2, \ldots, x_{d-1} .$$

(all x_i are distinct, every element of G is on the list).

Multiply with x:

$$xx_0, xx_1, xx_2, \ldots, xx_{d-1} .$$

Obviously, all these are elements of G.

Further, they are all different!

⌜ Assume $xx_i = xx_j$ for $i \neq j$.

then (dividing by x) $x_i = x_j$ ↯ . ⌟

Moreover, every element of G occurs on the second list.

⌜ Take x_i from the first list.

Now: $x^{-1}x_i$ is in G, so it's on the first list,

say $x^{-1}x_i = x_j$.

Then: $x_i = xx_j$ . . ⌟

Multiply the first list and multiply the second

ehc
29.4.08
4

so

$$x_0 \cdot x_1 \cdot \ldots \cdot x_{d-1} = xx_0 \cdot xx_1 \cdot \ldots \cdot xx_{d-1} \quad \text{in } G.$$

(Because G is commutative!)

Divide by $x_0 x_1 \cdot \ldots \cdot x_{d-1}$:

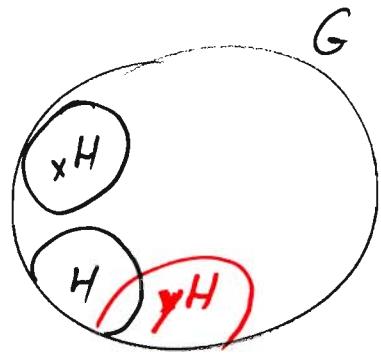
$$1 = \underbrace{x \cdot x \cdot \ldots \cdot x}_{d \text{ factors!}} = x^d.$$

because G is commutative. $\square$

Pf 2 In the non-commutative setting:

$$H < G \qquad (\text{i.e. } 1 \in H,\ \forall x,y \in H: x \cdot y \in H,\ \forall x \in H: x^{-1} \in H.)$$

Consider
$$G \longrightarrow G,$$
$$a \longmapsto xa.$$



It's bijective!

Thus $\#(xH) = \#H$.

Obviously: $G = \bigcup_{x \in G} xH$ since $1 \in H$.

Lemma: $xH \cap yH \neq \emptyset \Rightarrow xH = yH$.

$\ulcorner$ $a \in xH \cap yH$, ie $a = \underbrace{xh_1 = yh_2}$. $\to$ $x = y\underbrace{h_2 h_1^{-1}}_{\in H}$

Take $b \in xH$, ie. $b = xh$, then $b = y\underbrace{h_2 h_1^{-1} h}_{\in H} \in yH$.

Thus $xH \subset yH$. Similarly $yH \subset xH$. $\lrcorner$

So: $G = \dot{\bigcup}_{x \in T} xH$ for some set T, with each part of same size! $\Big\}$ $\#H \mid \#G$. $\square$

Let's apply that to $\mathbb{Z}_N^\times$, the unit group of integers modulo N.

ehc
29.4.08
5

<u>Thm</u> (Euler)

If x is coprime to N,
then
$$x^{\varphi(N)} = 1 \quad \text{in } \mathbb{Z}_N^\times$$
where
$$\varphi(N) := \# \mathbb{Z}_N^\times$$
is the Euler totient.

<u>Pf</u> Apply Thm (Lagrange) to $G = \mathbb{Z}_N^\times$. $\square$

<u>Thm</u> (Fermat's little theorem, 'fermat')

If $0 < x < p$ (or $p \nmid x$), p is prime
then
$$x^{p-1} = 1 \quad \text{in } \mathbb{Z}_p^\times.$$

<u>Pf</u> Apply Euler with $N = p$ and observe $\# \mathbb{Z}_p^\times = p-1$. $\square$

Compute:
$$3^{160} \quad \text{in } \mathbb{Z}_{101}^\times.$$

We know by fermat: $3^{100} = 1$ so we need
$$3^{160} \quad \text{in } \mathbb{Z}_{100}^\times.$$

ch c
29.4.08
6

We count: $\# \mathbb{Z}_{100}^{\times} = 40.$

Thus $3^{40} = 1$ in $\mathbb{Z}_{100}^{\times}$

so we need 160 in $\mathbb{Z}_{40}$

$$160 \equiv 0 \quad \text{in } \mathbb{Z}_{100}^{\times} \subset \mathbb{Z}_{100}$$

So

$$3^{160} = 3^{0} = 3^{1} = 3 \quad \text{in } \mathbb{Z}_{101}^{\times}.$$

Actually: we have

$$(\mathbb{Z}_{100}, +) \xrightarrow{\exp_3} (\mathbb{Z}_{101}^{\times}, \cdot)$$

$$\alpha \longmapsto 3^{\alpha}$$

is an isomorphism of groups! (if $3^{50} \neq 1$, $3^{20} \neq 1$.)

To see this we need: $3^{100} = 1$!

$$\alpha + \beta \longmapsto 3^{\alpha+\beta} \overset{?}{=} 3^{\alpha} \cdot 3^{\beta}$$

Yes, since $3^{100} = 1$

$$\alpha, \beta \longmapsto 3^{\alpha}, 3^{\beta} \longrightarrow 3^{\alpha} \cdot 3^{\beta}$$

$\boxed{\text{CRT}}$

$$\mathbb{Z}_{100} \cong \mathbb{Z}_4 \times \mathbb{Z}_{25}$$

numbers α w/.
$\alpha \equiv 0$ in $\mathbb{Z}_4$
$\alpha \equiv 1$ in $\mathbb{Z}_{25}$

To see

$$3^{160} = 3^{[2^{160}, 2^{160}]} = 3^{[0, 1^8]} = 3^{\underbrace{[0,1]}_{76}}$$

$$= 3^{76} = 71. \quad \text{in } \mathbb{Z}_{101}^{\times}.$$

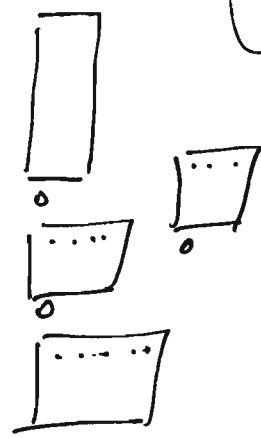
Startup example

A teacher has x pupils.

(#) in rows of 2: 1 remains

in rows of 3: 1 remain.

(*) $\begin{cases} \text{in rows of 4: 1 remains} \\ \text{in rows of 5: works!} \end{cases}$



How many pupils does he have?

Q: $x = ?$

Q: x unique!

Q: Does an x exist?

Guess and try $x = 25$:

$$\left.\begin{array}{l} x \equiv_5 0 \\ x \equiv_4 1 \end{array}\right\}$$
$$x \equiv_3 1$$
$$x \equiv_2 1 .$$

Let's reformulate (*):

$$x \equiv_4 1,$$
$$x \equiv_5 0.$$

$$x = 1 + s \cdot 4$$
$$\| $$
$$x = 0 + t \cdot 5$$

ie. $1 = s \cdot 4 + t \cdot 5$.

Use EEA(4,5) to find s, t and to check whether $\gcd(4,5) = 1$.

let's reformulate #:

$$x \equiv_2 1$$
$$x \equiv_4 1$$

As before that's:

$$x = 1 + s \cdot 2$$
$$= 1 + t \cdot 4$$

ie. $0 = s \cdot 2 + t \cdot 4$.

Since $0 = 1 - 1$ is divisible by $\gcd(2,4) = 2$ we can find a solution.

However if we change the task to

$$x \equiv_2 0$$
$$x \equiv_4 1.$$

$\Longleftrightarrow$ $\Longrightarrow$ $x \equiv_2 1$ ↯

the there is no solution

More complicated: $x \equiv_6 3 \Rightarrow x \equiv_2 1$ ↯

$x \equiv_{10} 4 \Rightarrow x \equiv_2 0$.

$\gcd(6,10) = 2$

General situation if the moduli $m_1, m_2 \in \mathbb{Z}$ are coprime: the task is to find $x \in \mathbb{Z}$ such that

$$x \equiv_{m_1} x_1,$$

$$x \equiv_{m_2} x_2.$$

for given $x_1, x_2 \in \mathbb{Z}$.

Translating this gives:

$$x = x_1 - \hat{s}\, m_1$$
$$= x_2 + \hat{t}\, m_2$$

i.e.

$$x_1 - x_2 = \hat{s}\, m_1 + \hat{t}\, m_2.$$

Now, assume that the EEA (m_1, m_2) returns:

$$1 = \underbrace{s\, m_1 + t\, m_2}.$$

Look at it modulo m_1:

$$1 \equiv_{m_1} t\, m_2$$

$$0 \equiv_{m_2} t\, m_2$$

$$\left| \begin{array}{lll} \boxed{t m_2} & \equiv_{m_1} & 1 \\ \underline{t m_2} & \equiv_{m_2} & 0 \end{array} \right| \cdot x_1$$

and the other way round:

$$1 \equiv_{m_2} s\, m_1$$

$$0 \equiv_{m_1} s\, m_1$$

$$\left| \begin{array}{lll} \boxed{s m_1} & \equiv_{m_1} & 0 \\ \underline{s m_1} & \equiv_{m_2} & 1 \end{array} \right| \cdot x_2$$

$$\Sigma$$

So consider:

$$x_0 := x_1 \cdot t m_2 + x_2 \cdot s m_1.$$

Check

$$x_0 \equiv x_1 \cdot \underbrace{t m_2}_{\equiv_{m_1} 1} + \underbrace{x_2 \, s m_1}_{\equiv_{m_1} 0} \equiv_{m_1} x_1$$

$$x_0 = \underbrace{x_1 \, t m_2}_{\equiv_{m_2} 0} + x_2 \underbrace{s m_1}_{\equiv_{m_2} 1} \equiv_{m_2} x_2 .$$

so it is a solution.

Notice: if x and x' are solutions

then $x - x' \equiv_{m_1} 0$ (ie. $m_1 \mid x - x'$)

$\equiv_{m_2} 0$ (ie. $m_2 \mid x - x'$)

further $\gcd(m_1, m_2) = 1$

ie, $x - x' \equiv_{m_1 \cdot m_2} 0$ so $m_1 m_2 \mid x - x'$.

And if x is a solution, so is $x + r \cdot m_1 m_2$.

Chinese Remainder Theorem (Down to earth version)

Given $m_1, m_2 \in \mathbb{Z}$ co prime

and $x_1, x_2 \in \mathbb{Z}$.

Then there exists $x \in \mathbb{Z}$ such that $x \equiv_{m_1} x_1$, $x \equiv_{m_2} x_2$.

and any two such solutions are equal modulo $m_1 \cdot m_2$. $\square$

Of course we have

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}_m, \\ x &\longmapsto x \bmod m. \end{aligned}$$

When is there a <u>nice</u> map

$$\mathbb{Z}_{m'} \longrightarrow \mathbb{Z}_m \quad ?$$

Let's try m', m coprime!

<u>Ex</u> $m' = 2, \quad m = 3.$

$$\begin{aligned} \mathbb{Z}_2 &\longrightarrow \mathbb{Z}_3 \\ 0 &\longmapsto 0 \\ 1 &\longmapsto 1 \\ 1+1=0 &\longmapsto 1+1 = -1 \neq 0 \\ &\longmapsto 0 \quad ↯. \end{aligned}$$

$$\begin{aligned} \mathbb{Z}_3 &\longrightarrow \mathbb{Z}_2 \\ 0 &\longmapsto \triangle 0 \\ 1 &\longmapsto 1 \\ -1 = 1+1 &\longmapsto 1+1 = \boxed{0} \\ 1+(-1) &\longmapsto 1 + \boxed{0} = 1 \\ \shortparallel \\ 0 &\longmapsto \triangle 0 \quad \neq ? \; ↯. \end{aligned}$$

Another guess:

$m' \mid m$

<u>Ex</u> $m' = 2,\ m = 4$:

$$\begin{array}{ccc} \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_4 \\ 0 & \longmapsto & 0 \\ 1 & \longmapsto & 1 \\ 1+1 & \longmapsto & 1+1 = 2 \\ \| & & \\ 0 & \longmapsto & 0 \end{array}$$

#↯

The other way round?

$m \mid m'$

<u>Ex</u>

$$\begin{array}{ccc} \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_2 \\ 0 & \longmapsto & 0 \\ 1 & \longmapsto & 1 \\ 2=1+1 & \longmapsto & 0 \\ 3=2+1 & \longmapsto & 1 \\ 1+1+1+1 & \longmapsto & 0 \\ \| & & \| \\ 0 & \longmapsto & 0 \end{array}$$

✓

Actually, this does it!

GAN:

ebonsenesenseenseense

$$\begin{tikzcd} 4\cdot\mathbb{Z} \arrow[d] \arrow[dr, "0"] & \\ \mathbb{Z} \arrow[d] \arrow[dr] & \\ \mathbb{Z}_4 \arrow[r, "?", "\exists!"'] & \mathbb{Z}_2 \end{tikzcd}$$

ehc
30.4.08
⑦

$m' = l \cdot m$.

Then there is a map

$$\begin{tikzcd}
\mathbb{Z} \arrow[d] \arrow[dr] & \\
\mathbb{Z}_{lm} \arrow[r] & \mathbb{Z}_m , \\
\bar{x} = x \bmod lm \arrow[r, mapsto] & x \bmod m .
\end{tikzcd}$$

Give x, x' with $x \bmod lm = x' \bmod lm$.

Then $x \bmod m = x' \bmod m$.

When we have a map

$$\mathbb{Z} \longrightarrow \mathbb{Z}_{lm} ,$$

then necessarily $lm \longmapsto 0$.

$$\begin{tikzcd}
m' \in \mathbb{Z} \arrow[d, dotted] & \\
\mathbb{Z}_{m'} \arrow[r] & \mathbb{Z}_m
\end{tikzcd}$$

Lemma There exists a ring map if and only if $m \mid m'$.

Pf

$$\begin{tikzcd}
0 \bmod m' \arrow[r, mapsto] \arrow[d, phantom, sloped, "="] & a \bmod m \\
m' \bmod m' \arrow[ur, mapsto] &
\end{tikzcd}$$

thus $(m' - 0) \bmod m = 0$

so $m' \bmod m = 0$, ie. $m \mid m'$. □

Consider

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \\ x &\longmapsto (x \bmod m_1,\ x \bmod m_2) \end{aligned}$$

Which elements map to zero?

Exactly the multiples of $m_1 m_2$.

(Assuming m_1, m_2 are coprime.)

Thus we get a ring map:

$$\begin{aligned} \mathbb{Z}_{m_1 m_2} &\longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \\ x \bmod m_1 m_2 &\longmapsto (x \bmod m_1,\ x \bmod m_2) \end{aligned}$$

Sideremark: $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ is a ring, of course.

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1,\ a_2 + b_2)$$

$$0 = (0, 0)$$

$$1 = (1, 1)$$

(We do not need any assumption on m_1, m_2 here.)

<u>Chinese Remainder Theorem</u> (Abstract version)

Given m_1, m_2 coprime then the map

$$\begin{aligned} \iota: \mathbb{Z}_{m_1 m_2} &\longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \\ \bar{x} = x \bmod m_1 m_2 &\longmapsto (x \bmod m_1,\ x \bmod m_2) \end{aligned}$$

is well-defined, injective and <u>surjective</u> ring morphism.

ehc
30.4.08
9

Apply it to count

$$\#\,(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2})^\times$$

By CRT we have

$$\mathbb{Z}_{m_1 m_2} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$$

thus

$$\mathbb{Z}_{m_1 m_2}^\times \cong (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2})^\times.$$

⌈ Notice: $x \in \mathbb{Z}_{m_1 m_2}^\times \iff \exists\, y \in \mathbb{Z}_{m_1 m_2} : xy = 1$

$$\iff \exists y \quad \underbrace{(x_1,x_2)}_{\overset{\shortparallel}{\iota(x)}} \cdot \underset{\overset{\shortparallel}{\iota(y)}}{(y_1,y_2)} = (1,1)$$

$$\cancel{\iff \exists\, y_1 \in \mathbb{Z}_{m_1}, y_2 \in \mathbb{Z}_{m_2} : x_1 \cdot y_1 = 1 \text{ in } \mathbb{Z}_{m_1},\ x_2 \cdot y_2 = 1 \text{ in } \mathbb{Z}_{m_2}}$$

$$\iff \exists (y_1,y_2) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} : \iota(x) \cdot (y_1,y_2) = (1,1).$$

⌋

Further:

$$(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_1})^\times = \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times$$

⌈ $(x_1,x_2) \in (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2})^\times$

$$\iff \exists\, (y_1,y_2) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} : (x_1,x_2)\cdot(y_1,y_2) = (1,1)$$

$$\iff \underbrace{\exists\, y_1 \in \mathbb{Z}_{m_1} : x_1 y_1 = 1 \text{ in } \mathbb{Z}_{m_1}}_{} \wedge \underbrace{\exists\, y_2 \in \mathbb{Z}_{m_2} : x_2 y_2 = 1 \text{ in } \mathbb{Z}_{m_2}}_{}$$

$$\iff x_1 \in \mathbb{Z}_{m_1}^\times \wedge x_2 \in \mathbb{Z}_{m_2}^\times$$

$$\iff (x_1,x_2) \in \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times$$

⌋

Together:

$$\mathbb{Z}_{m_1 m_2}^\times \cong \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times.$$

thus counting gives

$$\begin{array}{ccccc} \# \mathbb{Z}_{m_1 m_2}^{\times} & = & \# \mathbb{Z}_{m_1}^{\times} & \cdot & \# \mathbb{Z}_{m_2}^{\times} \\ \shortparallel & & \shortparallel & & \shortparallel \\ \varphi(m_1 m_2) & = & \varphi(m_1) & \cdot & \varphi(m_2) \end{array}$$

under assumption that m_1, m_2 are coprime.

$\mathbb{Z}_2 \backslash \mathbb{Z}_3$	0	1	2
0	0	4	2
1	3	1	5

$\leftarrow \mathbb{Z}_6$

$\mathbb{Z}_2 \backslash \mathbb{Z}_4$	0	1	2	3
0	0=4		2	
1		1		3

$\rightarrow \mathbb{Z}_2 \times \mathbb{Z}_4 \neq \mathbb{Z}_8$.

Similar:

$\mathbb{Z}_2 \times \mathbb{Z}_2 \neq \mathbb{Z}_4$.

In a ring $R_1 \times R_2$

obviously $(1,0) \cdot (0,1) = (0,0)$,

so that's a zero divisor.

Teacher needs a preimage under

$$\mathbb{Z}_{60} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$$

of $(1, 1, 0)$.

Now:

$$\begin{array}{ccc} \mathbb{Z}_{60} & \longrightarrow & \mathbb{Z}_3 \times \mathbb{Z}_{20} \\ ? & \longmapsto & (1, \bar{5}) \end{array}$$

$$\downarrow$$

$$\mathbb{Z}_4 \times \mathbb{Z}_5$$

$$(1, 0)$$

So: $1 = s \cdot 4 + t \cdot 5$ with $s = -1$, $t = 1$. (by EEA ☺).

Thus $5 \equiv_4 1$ $\quad -4 \equiv_4 0$

$\equiv_5 0$ $\quad \equiv_5 1$

and so $5 = 1 \cdot 5 + 0 \cdot (-4) \equiv_4 1 \cdot 1 + 0 \cdot 0 = 1$

$\equiv_5 1 \cdot 0 + 0 \cdot 1 = 0$

Further: $1 = s' \cdot 3 + t' \cdot 20$ with $s' = 7$, $t' = -1$ by EEA ☺.

Thus $-20 \equiv_3 1$ $\quad 21 \equiv_3 0$

$\equiv_{20} 0$ $\quad \equiv_{20} 1$

so $\underline{85} = 1 \cdot (-20) + 5 \cdot 21 \equiv_3 1 \cdot 1 + 5 \cdot 0 = 1$

$\equiv_{20} 1 \cdot 0 + 5 \cdot 1 = \underline{5}$

$\equiv_4 5 \equiv_4 1$

$\equiv_5 5 \equiv_5 0$.

Thus our solution is $\boxed{25 \bmod 60}$.

<u>Corollary</u> p, q two different primes

$$\varphi(p \cdot q) = (p-1) \cdot (q-1).$$

$\square$

RSA

<u>Setup</u> Choose p, q prime, different. (Large!)

<u>Toy Ex</u>: $p = 5, q = 7$.

Compute $N = p \cdot q$ ring size

Compute $L = (p-1)(q-1)$ repetition length.

Further choose two numbers $e, d < L$

such that $ed \equiv_L 1$.

Now: (N, e) ~~is~~ the public key,

(N, d) is the private key.

Forget everything else (asap)!

<u>Encrypt</u> Input: x a plaintext.

Output: $y = x^e$ in $\mathbb{Z}_N$.

<u>Decrypt</u> Input: y a ciphertext.

Output: $z = y^d$ in $\mathbb{Z}_N$.

Next time: PCES?

RSA

Setup

say 512-bit numbers

p, q prime numbers, $p \neq q$,

$N = p \cdot q$, $L = (p-1)(q-1) = \varphi(N)$

$e, d \in \{1, \dots, L-1\}$ s.t. $ed \equiv_L 1$. (EEA)

Public key (N, e), private key (N, d)

Encrypt $x \longmapsto y = x^e$ in $\mathbb{Z}_N$

Decrypt $y \longmapsto z = y^d$ in $\mathbb{Z}_N$

$\boxed{\text{PCES?}}$ P ✓

C: $z = x$? $\quad z = y^d = (x^e)^d = x^{ed} = x$

Proof 1 Case $(x,N)=1$: Because $x^L = 1$ in $\mathbb{Z}_N^\times$ and

$ed = 1 + kL$, so

$x^{ed} = x^1 \cdot (\underbrace{x^L}_{1})^k = x$. □

$\text{prob}((x,N) \neq 1) = \frac{p+q-1}{pq} \approx 2^{-511} \approx 0$

Remaining case very improbable.

Proof 2 General case: Note that $x^{p-1} = 1$ in $\mathbb{Z}_p^\times$. (Fermat)

(So $x^p = x$ in $\mathbb{Z}_p$.)

Or: Thus $x^{1+k(p-1)} = x$ in $\mathbb{Z}_p$ for $k \geq 0$.

So we obtain using $ed = 1 + \underbrace{k(q-1)}(p-1)$

that $x^{ed} = x$ in $\mathbb{Z}_p$.

Also $x^{ed} = x$ in $\mathbb{Z}_q$.

Thus $x^{ed} = x$ in $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_N$. □

E? p, q : $n/2$ tries to find a $n/2$-bit prime, prime test $O(n^3)$, $\ln(n)$ often

N, L : 2 multiplications of $n/2$-bit numbers $\Big\}\ O(n^2)$

e, d : EEA (twice)

etc 6.5.08 ②

setup $\in \tilde{O}(n^4)$

Encrypt/decrypt $O(n^3)$

Prime Number Theorem

$$\pi(x) := \#\{ N \in \mathbb{N}_{\leq x} \mid N \text{ prime} \}$$

Then

$$\frac{\pi(x)}{x} \approx \frac{1}{\ln x} = \frac{\log_2 e}{\log_2 x}$$

Probability for a number chosen in $\mathbb{N}_{<x}$ to be prime

more precisely for $x \geq 100$

$$\frac{1}{\ln x}\left(1 + \frac{1}{2}\frac{1}{\ln x}\right) \leq \frac{\pi(x)}{x} \leq \frac{1}{\ln x}\left(1 + \frac{3}{2}\frac{1}{\ln x}\right)$$

Everything is expected poly-time.

S? ① $N \mapsto (p, q)$ Factorization is ~~probably~~ possibly difficult.

② $N \mapsto L$

③ $(N, e) \mapsto d$

④ $(N, e, y) \mapsto x$ (? OPEN!)

Solution to ② $\Rightarrow$ Solution to ①

Consider $(x-p)(x-q) = x^2 - (N-L+1)x + N$.

$\left\{ \begin{array}{l} (N,e) \mapsto d \\ (N,e') \mapsto d' \end{array} \right.$ then $\gcd(\underbrace{ed-1}_{2n\text{-bit}}, \underbrace{e'd'-1}_{2n\text{-bit}})$ a small multiple of φ with high prob.

Excursion

LOOP: repeat
sth
until condition

Know: prob(condition) = p.

What is the expected number R of executions of "sth"?

$q := 1-p$

$$p \cdot 1 + q \cdot (p \cdot 2 + q \cdot (p \cdot 3 + q \cdot \ldots$$

$$p + qp \cdot 2 + q^2 p\, 3 + q^3 p\, 4 + \ldots$$

$$E(R) = \sum_{i=1}^{\infty} p\, q^{i-1} i$$

$|q| < 1$

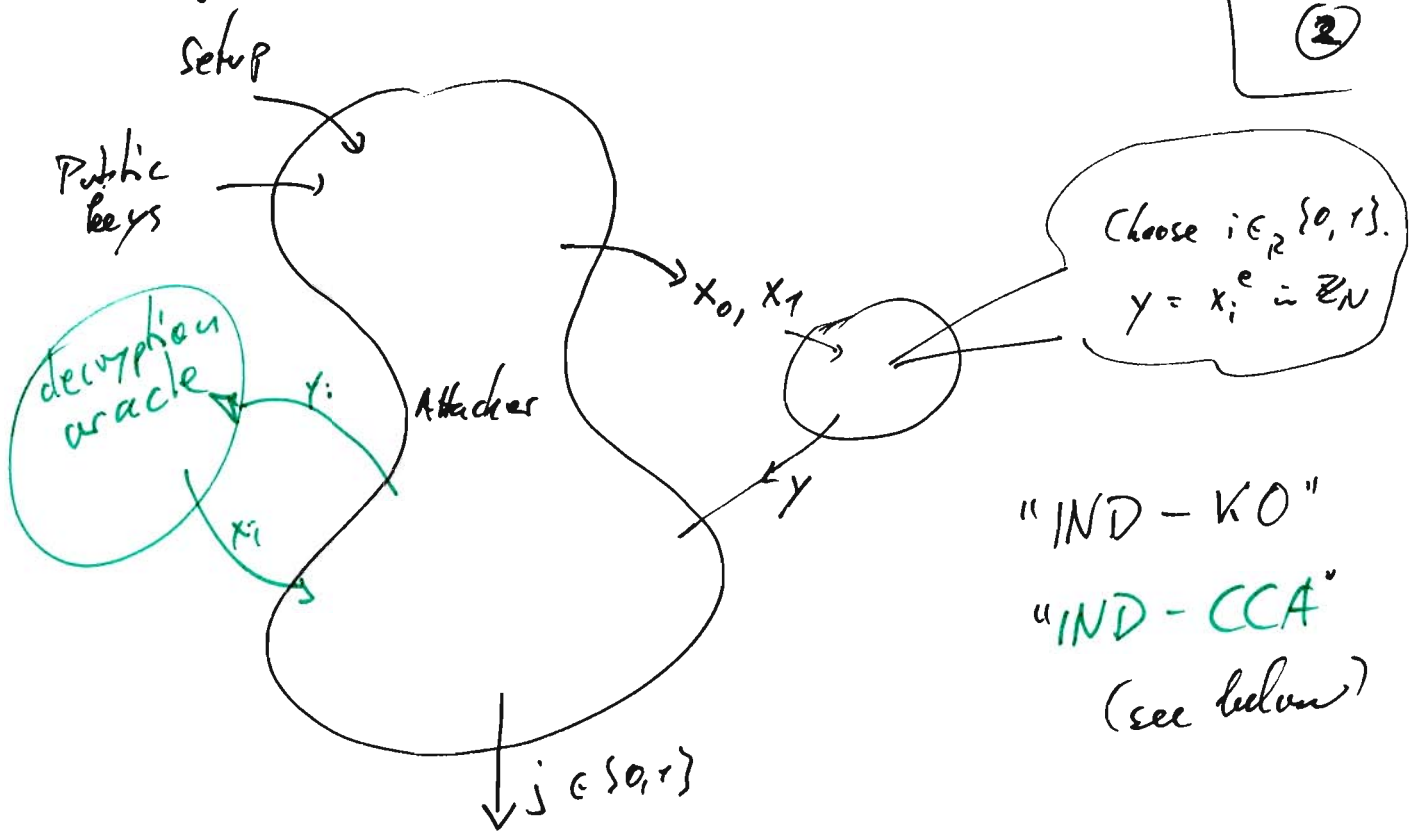
$$\begin{array}{r|l} s & 1+q+q^2+\ldots \\ -qs & q+q^2+\ldots \\ \hline (1-q)s & 1 \end{array}$$

$$= p \underbrace{\sum_{i=0}^{\infty} i q^{i-1}}$$

$$= \left(\underbrace{\sum_{i=0}^{\infty} q^i}\right)' = \left(\frac{1}{1-q}\right)' = \frac{+1}{(1-q)^2}$$

$$= \frac{p}{p^2} = \frac{1}{p}. \quad \checkmark$$

Security goal? (for encryption)



"IND-KO"

"IND-CCA" (see below)

Attacker's goal: $j = i$.

Our goal: $\forall$ attacker: prob$(j = i)$ negligible away from guessing (very small)

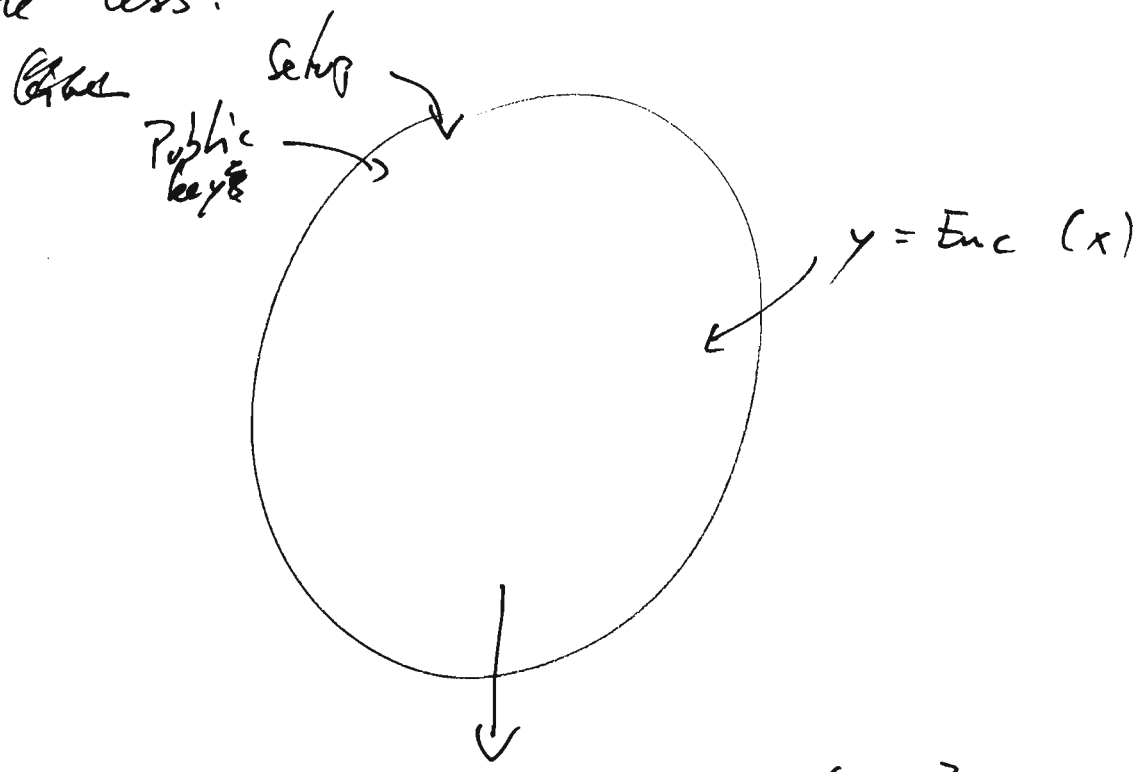
Actually, this cannot hold for RSA

because $y_0 = x_0^e$ in $\mathbb{Z}_N$

$y_1 = x_1^e$ in $\mathbb{Z}_N$

so the attacker simply chooses j s.t. $y = y_j$.

A little less:



$b : \mathbb{Z}_N \to \{0,1\}$

$\mathbb{Z}_N = \{0, \dots N-1\}$

~~$b(x)$~~

$j \in \{0,1\}$

Attacker's goal: $b(x) = j$.

Our goal: $\forall$ attacker: prob$(b(x) = j)$ close to guessing.

RSA has that for some b given that decryption (4) is difficult

For example: $b_0(x) = \hat{x} \bmod 2 =: x_0$

<u>Thm</u> If we can compute $b_0(x)$ from N, e, y then we can compute x from N, e, y. (Ex)

Such a function is called a hard-core bit.

Signatures

ElGamal signatures ('80?)

Verify

$$(*) \qquad a^{b^*} \, b^{\gamma} = g^{h(m)} \quad \text{in a group } G$$

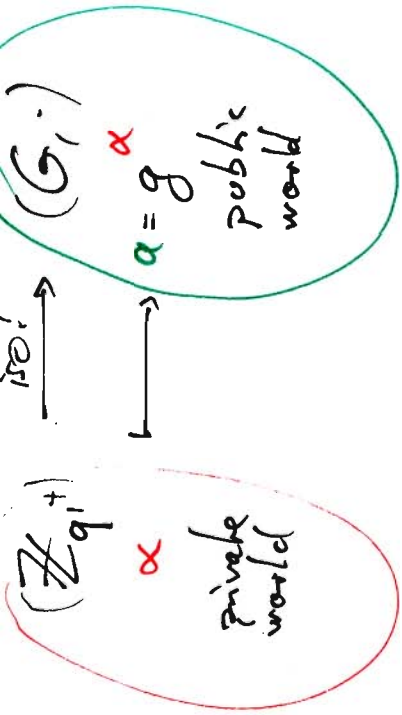
Analogy: $G \ni g$ a group with an element of high (prime) order:

Setup

$g^q = 1$ for some large prime q.

(size$(q) \approx 160$, ?

if $G = \mathbb{Z}_p^\times$ then size$(p) \approx 1024$.)



$*: G \to \mathbb{Z}_q$ some easy function.

h is a hash function, like

MD5, SHA-1, RIPEMD160 $\in \{0,1\}^{160}$,

completely broken broken!

SHA-2: SHA-224, SHA 256, ..., SHA512

a is the public key of the signer

$$a = g^{\alpha}.$$

Sign: Rewrite $(*)$:

$$g^{\alpha b^* + \beta \gamma} = g^{h(m)} \text{ in } G.$$

using $b = g^\beta$

Equivalent: $\alpha b^* + \beta \gamma = h(m)$ in $\mathbb{Z}_q$.

ekc
7.5.08
5

Sign

Input: Setup, m document

Output: (b, γ) signature

1. Choose $\beta \in_R \mathbb{Z}_q^*$.
2. Compute $b = g^\beta$ in G.
3. Solve $\alpha \underline{b}^* + \beta \gamma = \underline{h}(m)$ in $\mathbb{Z}_q$ for γ.
4. Return (b, γ).

Actually this is a generalization of the original ElGamal proposal. He used $q = p - 1$ (not prime!).

We can also use an elliptic curve for G!

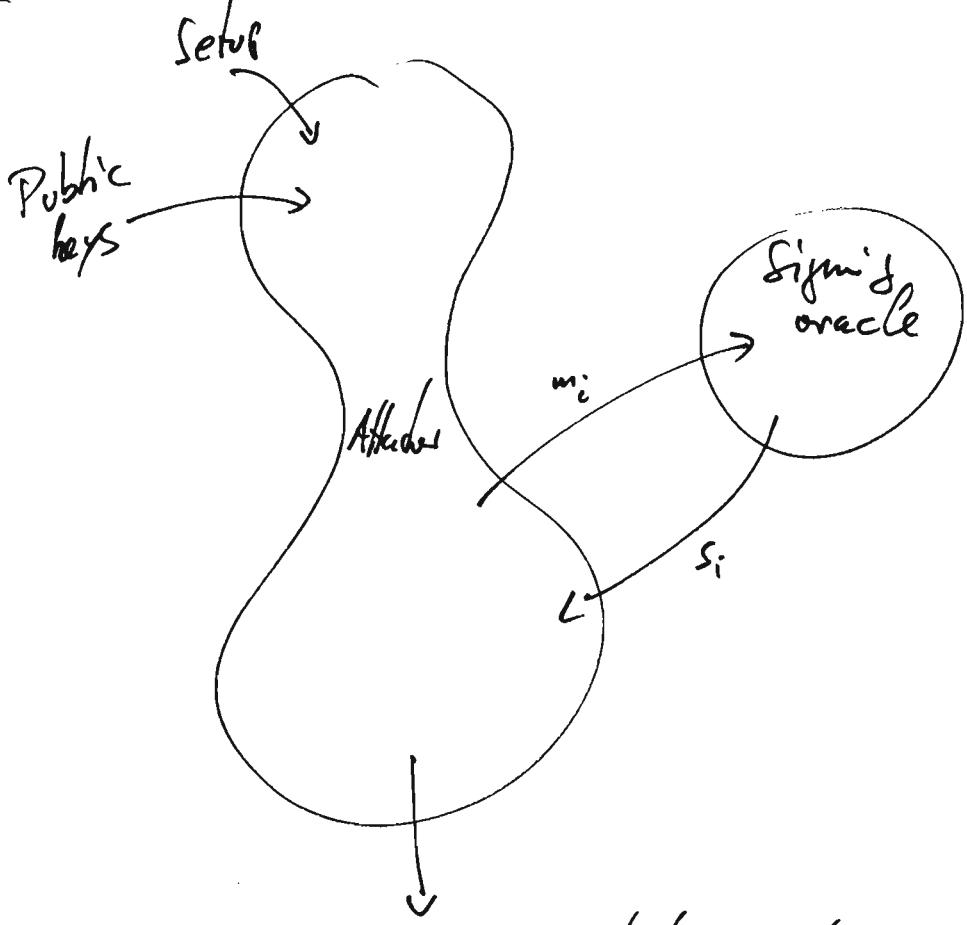
P ✓

E: all polynomiale ✓ (also fast in practice) ✓

C: Verify(m, Sign(m)) = TRUE by construction.

S: ?

Security goal? (for signatures)



(m, s) ~~valid signed~~

Attacker's goal: s is a signature to m, but m is none of the m_i.

Our goal: $\forall$ attacker: prob(Verify(m, s)) is close to guessing (20)

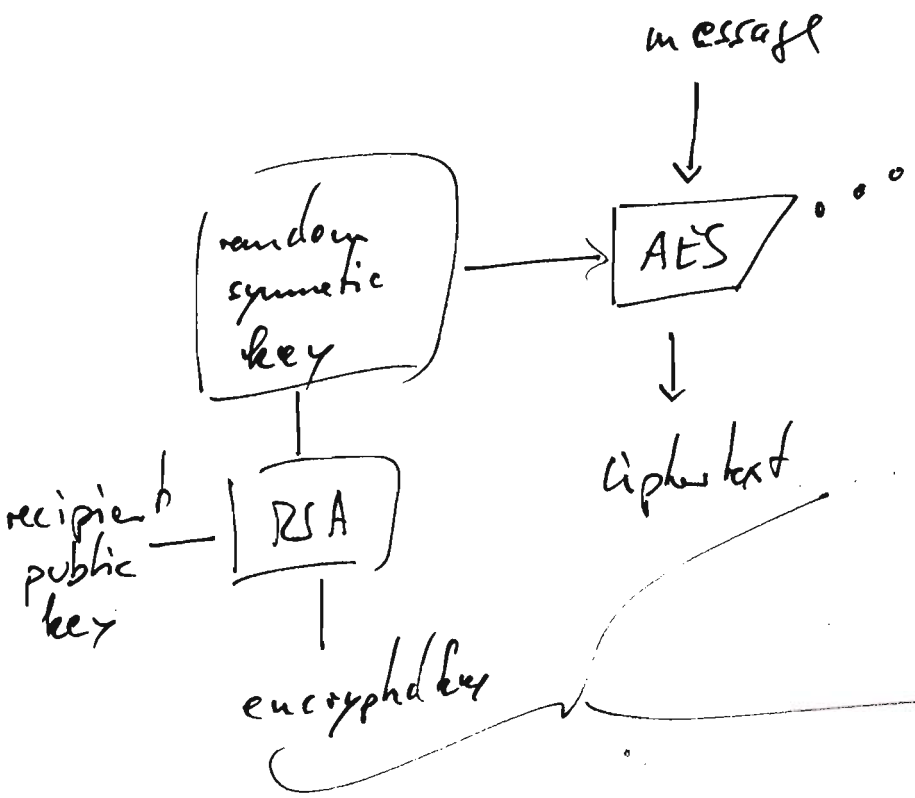
Overview and how it's done in practice

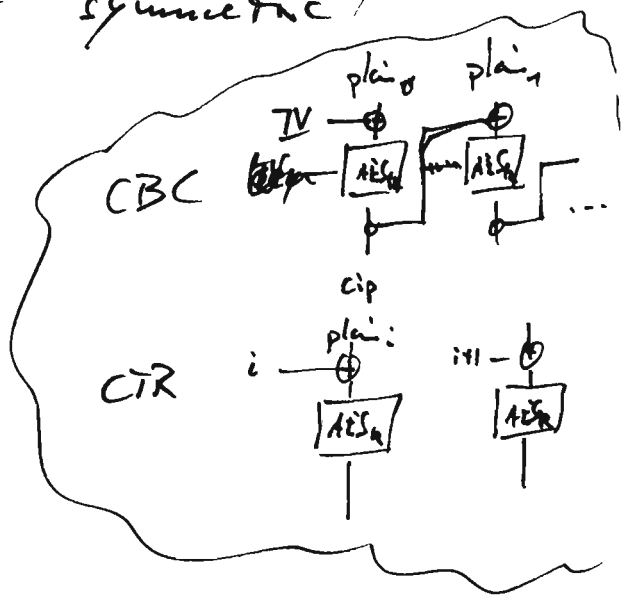
ehc
20.5.08
1

Encryption (for secrecy):

RSA – private/public – asymmetric /ElGamal encryption

(AES – secret – symmetric)





Signatures (for integrity and authenticity):

ElGamal signatures (p/p – asymmetric) /RSA signature

$\boxed{a^{b^* b^{\gamma}} = g \text{ in } G}$ $h(x)$

$\alpha b^* + \beta\gamma$ $h(x)$

g $= g$

$\exp_g : \mathbb{Z}_{\mathrm{ord}(g)} \cong \langle g \rangle$

$0, \dots, q-1$ $g^0, g^1, \dots, g^{q-1}$

$q = \mathrm{ord}(g)$, $g^q = 1$

$\alpha b^* + \beta\gamma = h(x) \text{ in } \mathbb{Z}_q$

(MAC)

Excursion on DL

In ~~the~~ any group G: We try to solve $g^{\alpha} = a$ in G.
for α.

Write $\alpha = \alpha_1 r + \alpha_0$ with α_1, α_0 of same length
so that $r^2 > \mathrm{ord}(g)$.

Compute $a\, g^{-\alpha_0}$ for $\alpha_0 \in \{0, \dots, r-1\}$.
(baby steps)

Compute $g^{\alpha_1 r}$ for $\alpha_1 \in \{0, \dots, r-1\}$

and try to find it among the baby steps.
(giant steps)

Given a solution $g^{\alpha_1 r} = a\, g^{-\alpha_0}$

we have $g^{\underbrace{\alpha_1 r + \alpha_0}} = a$.

Time & Space: $\sqrt{\mathrm{ord}(g)} = \sqrt{\#\langle g\rangle} = \tilde{O}(2^{n/2})$

In $\mathbb{Z}_p$ we can do better!

Reason: we have $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_p$
and in $\mathbb{Z}$ we have a unique prime factorization.

We try to solve $g^s a = \underline{p_1}^{e_1} \cdot \ldots \cdot \underline{p_r}^{e_r}$
$= g^{s_1 e_1} \cdot \ldots \cdot g^{s_r e_r} = g^{s_1 e_1 + \ldots + s_r e_r}$

by first finding small primes $p_1, \dots, p_r$ with their discrete logs.
We do this by using random numbers s_i and trying to factor $g^{s_i} \bmod p = p_1^{f_{i1}} \cdot \ldots \cdot p_r^{f_{i r}} \cdot 1$.

$\exp\left(O(1) \cdot n^{1/2} (\log n)^{1/2}\right)$

ElGamal encryption

enc: Input: msg x, public key a, setup (G,g)
Output: ciphertext (t, y)

1. Choose $\tau \in_R \mathbb{Z}_q^+$.
2. Compute g^τ in G.
3. Compute $a^\tau \cdot x$ in G.
4. Return $(g^\tau, a^\tau \cdot x)$

dec: Input: (t,y) ciphertext, private key α, setup with $a = g^\alpha$
Output: plaintext x
1. Return y / t^α.

Setup: (G,g) a DLP-proof group with element g.
Public/private key pair: $a = g^\alpha$.

Note that
$$\underbrace{(g^\tau)^\alpha}_{t^\alpha} = \underbrace{(g^\alpha)^\tau}_{a^\tau}$$

The encryption attacker has to spot a difference between:

(t, y) which is the encryption of x_0 or x_1. under public key a.

$$\begin{array}{cccc} (g, & g^\alpha, & g^\tau, & g^\xi) \\ \uparrow & \uparrow & \uparrow & \uparrow \\ g & a & t & y/x_i \end{array} \longmapsto \text{TRUE / FALSE answering } \xi = \alpha\tau \text{ ?}$$

Decisional Diffie-Hellman Problem

[IND-KO]

<u>Thm</u> The attacker can break DDH iff he can break ElGamal enc. w/o access to decryption oracle.

How to machify an Elgamal encryption?

ehc 20.5.08 (4)

$$(t, y) \xmapsto[\text{re-encryption}]{?} (t', y')$$

$$\downarrow \qquad\qquad \downarrow$$

$$y/t^{\alpha} = x \qquad\qquad y'/t'^{\alpha} = x$$

$$t' = g^{\rho}\, t \quad \left(= g^{\rho} g^{\tau} = g^{\overbrace{\tau+\rho}^{=:\tau'}} \right)$$

$$y' = a^{\rho} \cdot y \quad \left(= \underbrace{a^{\rho}(a^{\tau} \cdot x)}_{(a^{\rho} \cdot a^{\tau}) \cdot x} = a^{\overbrace{\tau+\rho}^{\tau'}}\, x \right)$$

$$\frac{y'}{t'^{\alpha}} = \frac{a^{\rho} y}{(g^{\rho} t)^{\alpha}} = \underbrace{\frac{g^{\alpha\rho}}{g^{\rho\alpha}}}_{=1!} \frac{y}{t^{\alpha}}$$

---

ehc 21.5.08 (1)

Thus Elgamal encryption does <u>not</u> fulfill the strongest security goal ~~sent~~ versus an attacker with access to a decryption oracle. [IND - CCA]

for the attacker's task, namely to distinguish two encrypted message

Chosen-Ciphertext-Attack

Pf Attacker: Choose $x_0, x_1 \in G$ different.
It queries an encryption (t, y) of one of them.
Then reencrypts this to (t', y')
and calls the decryption oracle on it to get x'.
If $x' = x_0$ answer 0, if $x' = x_1$ answer 1.

Rescue: Use ElGamal encryption with 'mixed' operation:

$$x \xmapsto{r \in_R \mathbb{Z}_q} (g^r, a^r \diamond x)$$

for example: $a^r \underset{\text{XOR}}{\oplus} x$

or: $h(a^r) \underset{\text{XOR}}{\oplus} x$

Then no reencryption seems possible.

Actually, in the random oracle model we then have:

ElGamal encryption is IND-CCA secure in the ROM iff DDH is difficult

---

RSA signatures

Verify: $\boxed{h(x) = s^e \text{ in } \mathbb{Z}_N}$

Setup: as with RSA $\rightarrow$ (N, e) public, (N, d) private.

Sign: $s \leftarrow h(x)^d$, return (x, s).

Thm RSA signature with $h = id$ does not fulfill the security goal for signatures. Ex

<u>Claim:</u> RSA signature with a hash function that is surjective on $\mathbb{Z}_N$ does fulfill the security goal in the random oracle model.

Let's assume the RSA signature with a certain function $h: \{0,1\}^* \longrightarrow \mathbb{Z}_N$.

What property on h does that imply?

(1) Assume the attacker <u>can compute</u> a preimage for h. (efficiently)

<u>Attacker 1</u>

Input: setup & keys (N, e)

Output: (x, s)

Aim: $h(x) = s^e$ in $\mathbb{Z}_N$.

1. Choose $s \in_R \mathbb{Z}_N$.
2. Compute a preimage x of s^e under h, so $h(x) = s^e$ in $\mathbb{Z}_N$.
3. Return (x, s)

This attacker breaks the security goal!

<u>Thm</u> If RSA-sign(h) is secure then <u>h is one-way</u>.

(2) Assume the attacker can find two different documents with same hash. (efficiently)

ehc 21.5.08 (4)

Attacker 2

Input: setup & keys (N, e)

Output: (x, s)

Sim: $h(x) = s^e$ in $\mathbb{Z}_N$ // verify(x,s) = TRUE

1. Find two documents x_0, x_1 with $x_0 \neq x_1$ and $h(x_0) = h(x_1)$.
2. Query the signing oracle for a signature s on x_1.
3. Return (x_0, s).

This attacker breaches the security goal!

Thm (i) If RSA-sign(h) is secure then h is collision-resistant.

(ii) For any signature scheme that only works with an h-hash of the document we have: if it's secure then h is collision-resistant.

NOTE: By chosing documents at random we expect to find a collision after $O(\sqrt{\#\text{possible hashes}})$ steps.

→ SHA1 is a practical hash function

$$\{0,1\}^* \longrightarrow \{0,1\}^{160}.$$

(see Wikipedia (en + SHA_hash_functions)

State of the art:

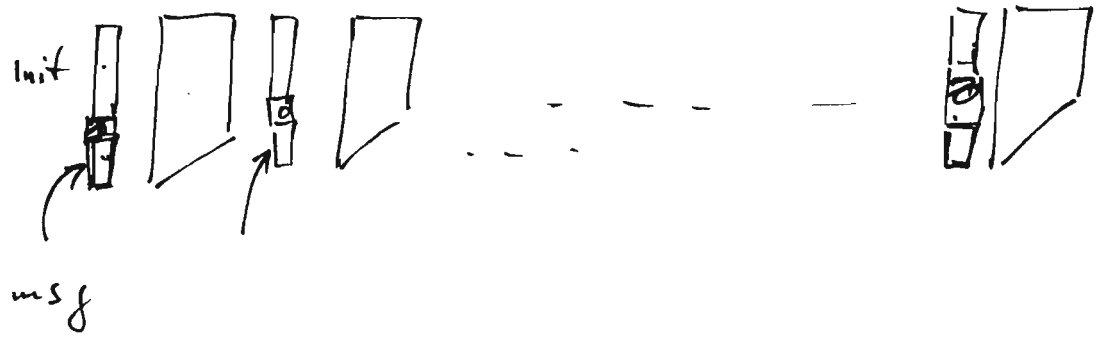
MD4	→ 128 bits	BROKEN (2 calls!)
MD5	→ 128/160 bits?	BROKEN (few seconds)
SHA1	→ 160 bits	2^{63} attack, broken

others: SHA256, ...

A 'provably' secure hash function is built from:

$$\mathbb{Z}_q \times \mathbb{Z}_q \longrightarrow G \qquad \left\{ \begin{array}{l} * \longrightarrow \mathbb{Z}_q \\ \longmapsto (g^{\alpha} h^{\beta})^{*} \end{array} \right.$$

$$\underbrace{(\alpha, \beta)}_{2n \text{ bits}} \longmapsto \underbrace{g^{\alpha} h^{\beta}}_{n \text{ bits}}$$



This gives a ~~[illegible]~~ one-way and collision-resistant function provided the DL in G is difficult.

But: much too slow in practice!

Exam about 22 - 28 August

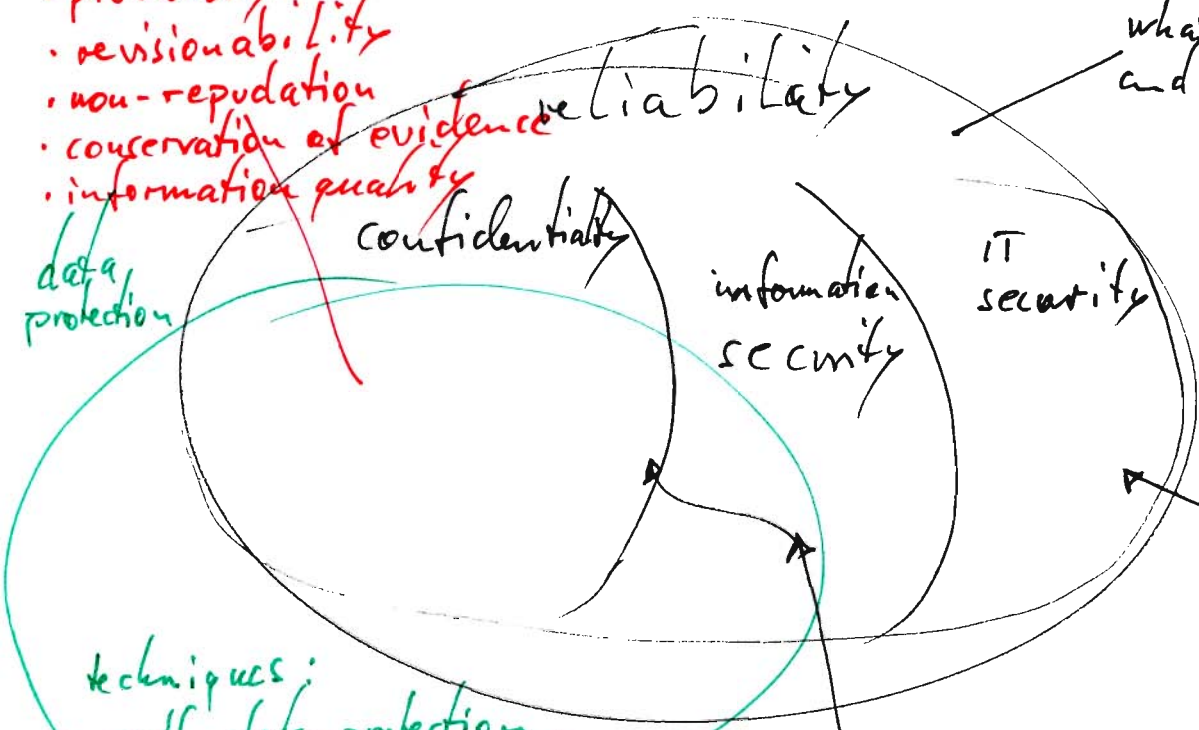
deadline

ehc 20.5.08 (1)

Requirements

- freedom of insured people, rights
  - data protection
    - The insured must be able to decide which of their data is stored, deleted, and accessed.
    - The insured have information and reading rights on their own data and the associated processes.

manageability
- responsibilities
- usage rules
- provability
- revisionability
- non-repudation
- conservation of evidence
- information quality



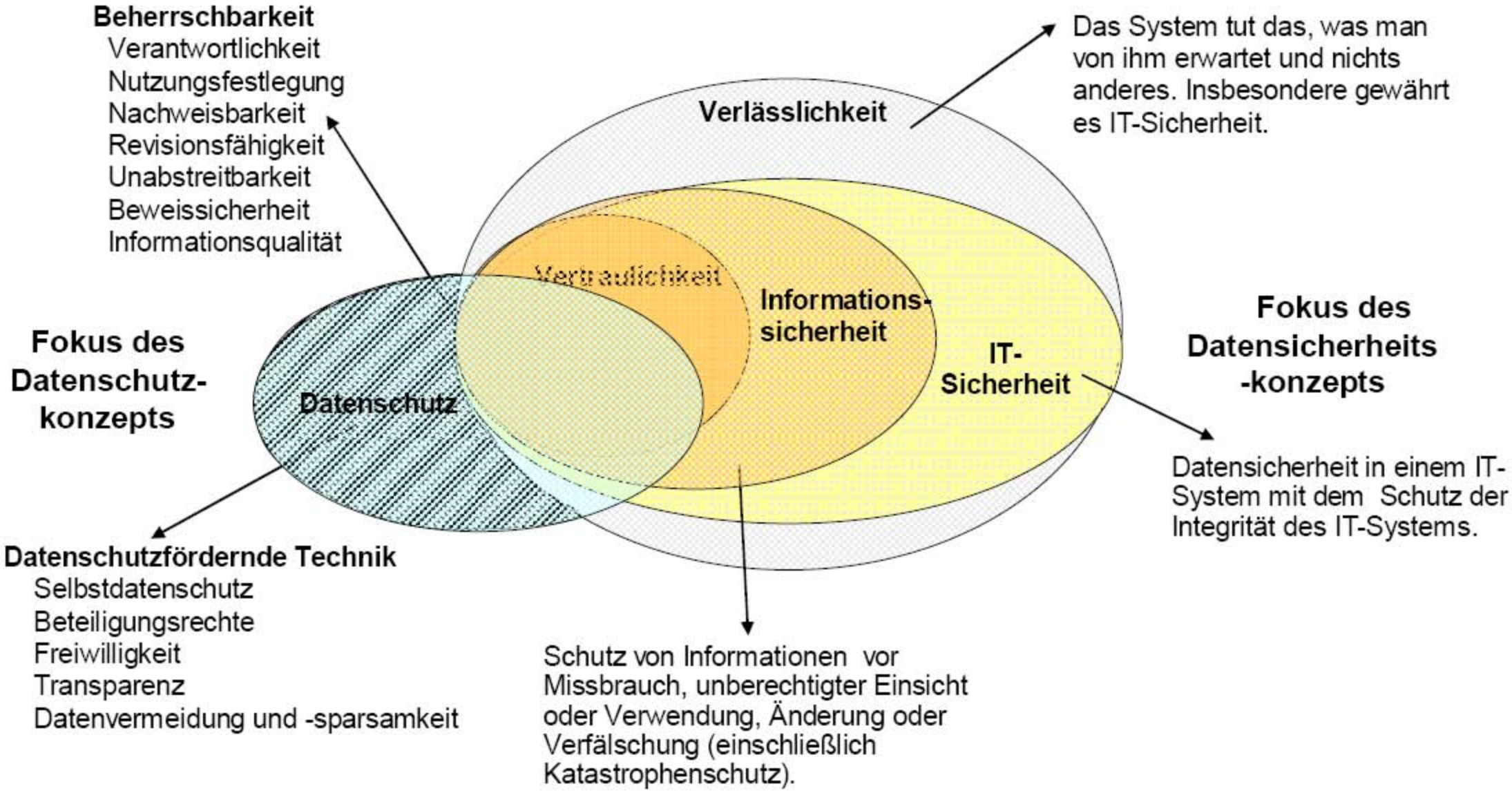
The system does what it should and nothing else.

data security

The integrity of the system should be assured

techniques:
- self data protection
- participation right
- voluntarity
- transparency
- data avoidance & data ~~space~~ thrift (?)

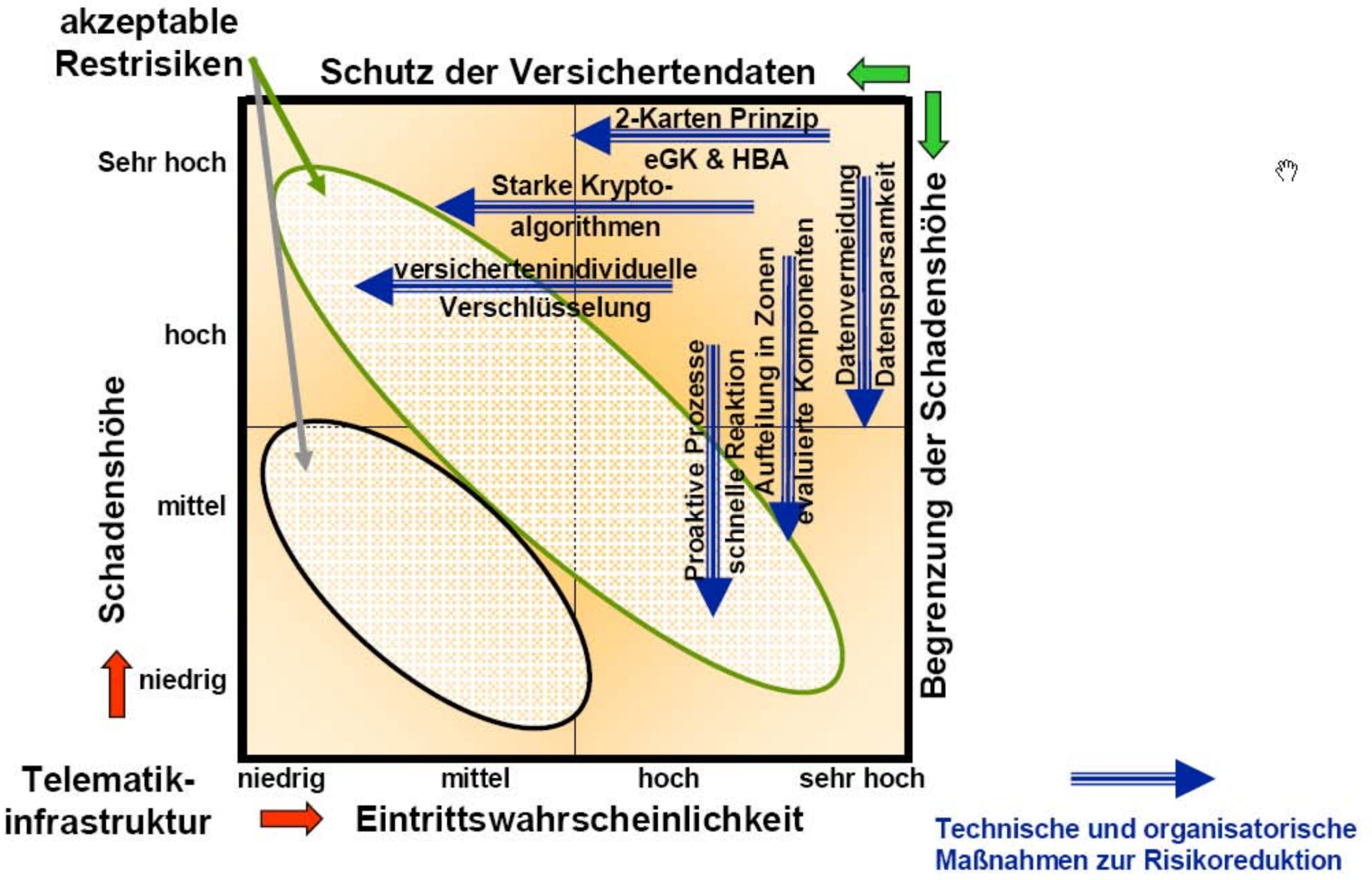
protection from abuse, unauthorized access or use (including emergency protection)

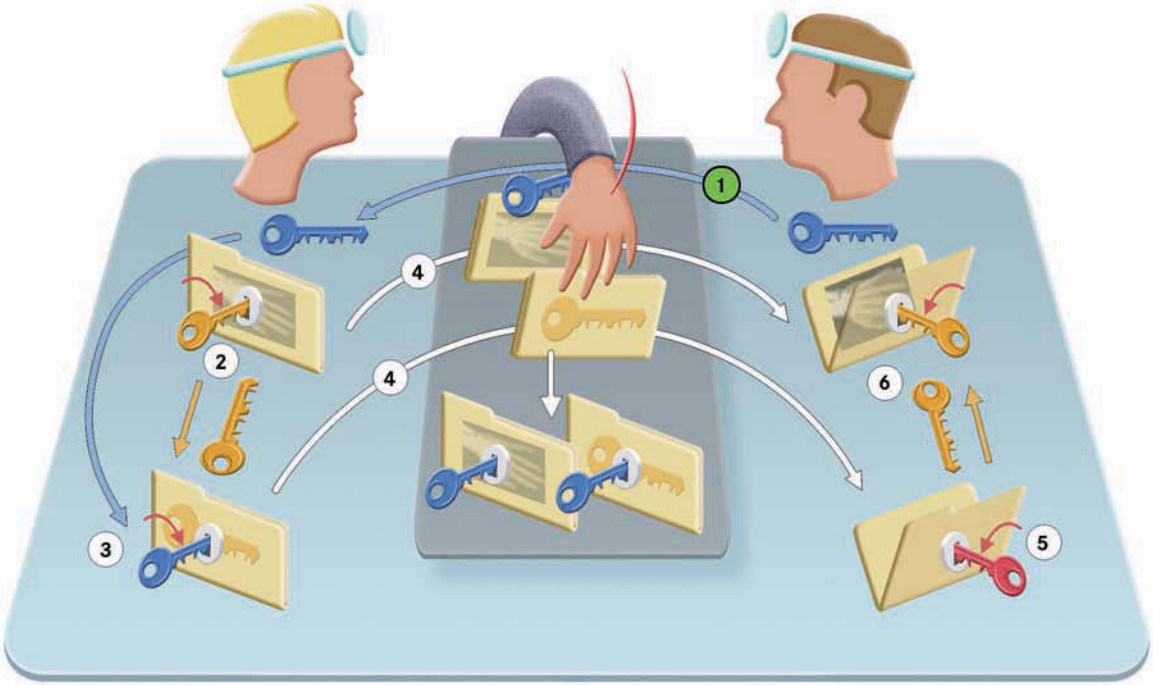

Beherrschbarkeit
Verantwortlichkeit
Nutzungsfestlegung
Nachweisbarkeit
Revisionsfähigkeit
Unabstreitbarkeit
Beweissicherheit
Informationsqualität
Verlässlichkeit
Das System tut das, was man von ihm erwartet und nichts anderes. Insbesondere gewährt es IT-Sicherheit.
Vertraulichkeit
Informations-sicherheit
IT-Sicherheit
Datenschutz
Fokus des Datenschutz-konzepts
Fokus des Datensicherheits-konzepts
Datensicherheit in einem IT-System mit dem Schutz der Integrität des IT-Systems.
Datenschutzfördernde Technik
Selbstdatenschutz
Beteiligungsrechte
Freiwilligkeit
Transparenz
Datenvermeidung und -sparsamkeit
Schutz von Informationen vor Missbrauch, unberechtigter Einsicht oder Verwendung, Änderung oder Verfälschung (einschließlich Katastrophenschutz).

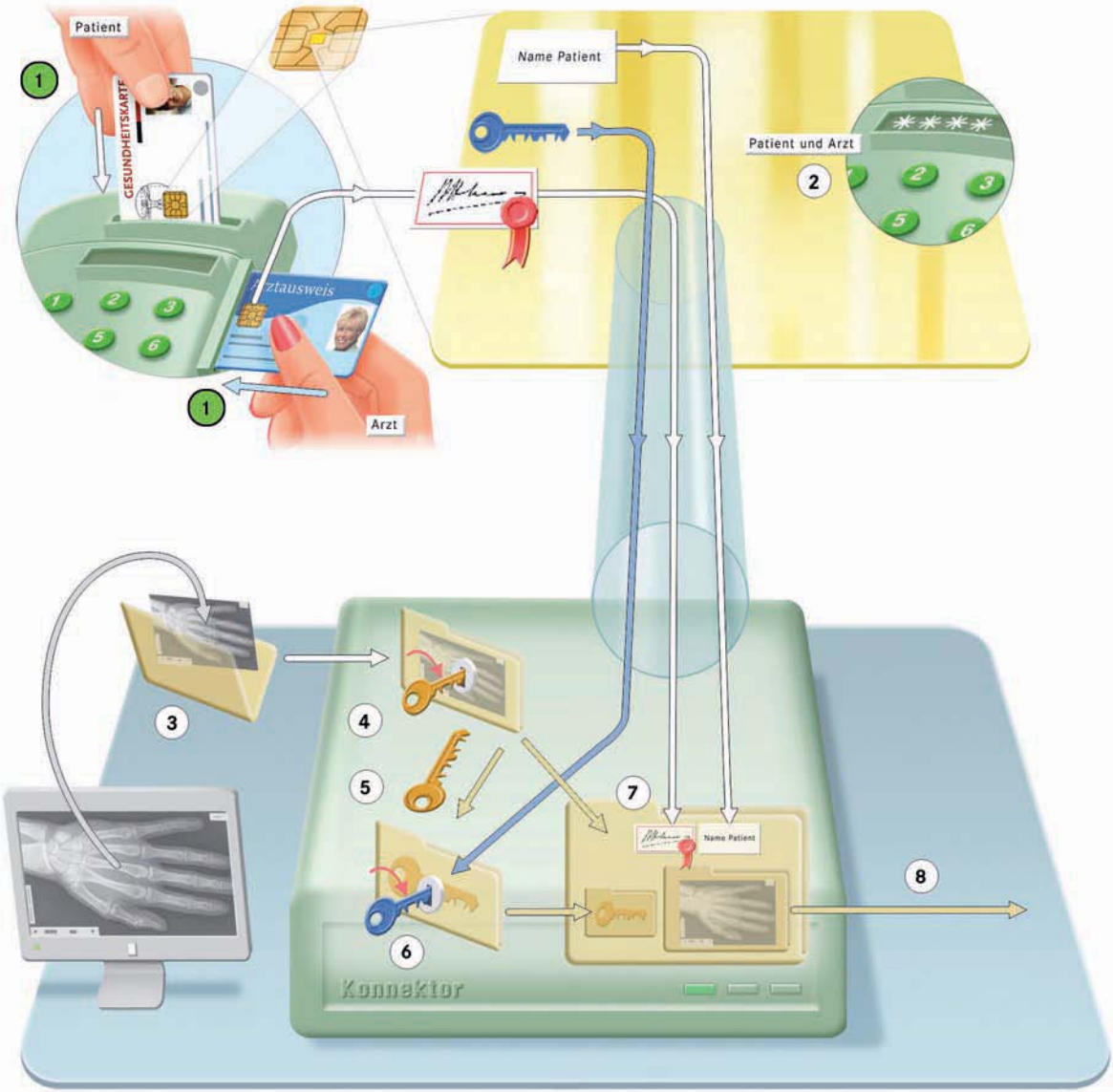
Threats to the health care infrastructure

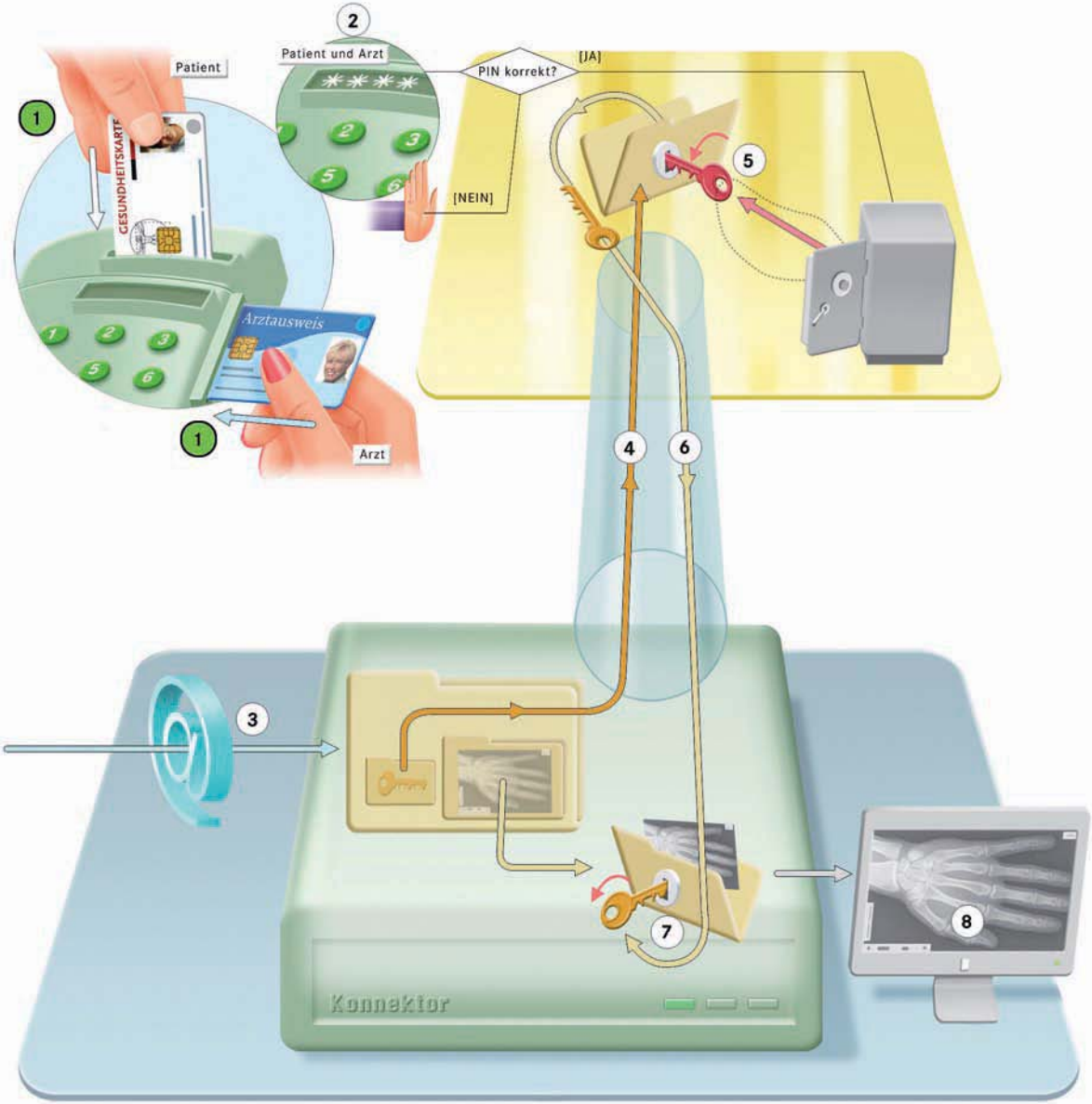
Four groups

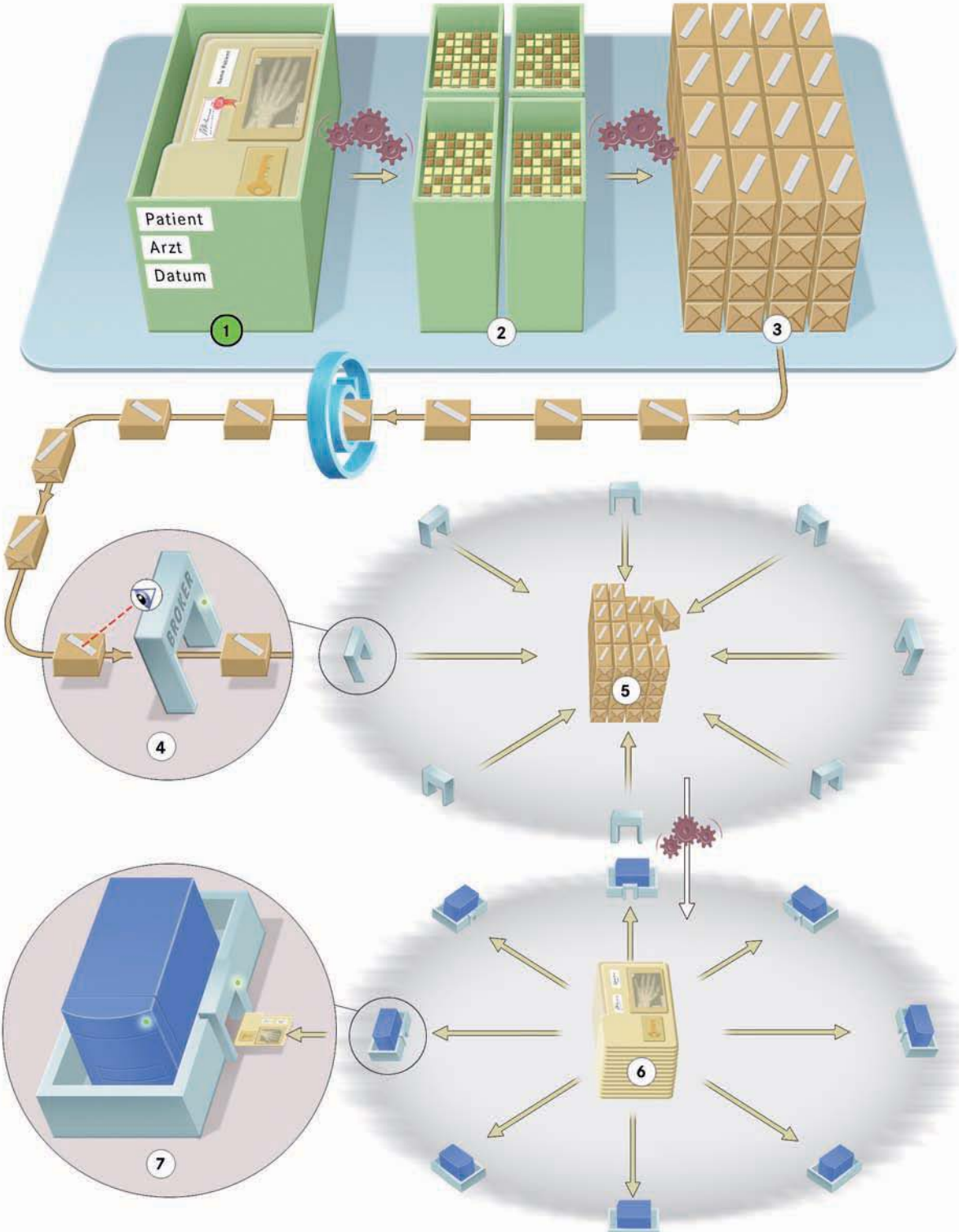
- from Users
- from Admins
- from Attackers
- from Hardware / Software


akzeptable Restrisiken
Schutz der Versichertendaten
2-Karten Prinzip
eGK & HBA
Starke Krypto-algorithmen
versichertenindividuelle Verschlüsselung
Proaktive Prozesse
schnelle Reaktion
Aufteilung in Zonen
evaluierte Komponenten
Datenvermeidung
Datensparsamkeit
Begrenzung der Schadenshöhe
Schadenshöhe
Sehr hoch
hoch
mittel
niedrig
Telematik-infrastruktur
niedrig
mittel
hoch
sehr hoch
Eintrittswahrscheinlichkeit
Technische und organisatorische Maßnahmen zur Risikoreduktion


1
2
3
4
4
5
6


Patient
1
GESUNDHEITSKARTE
Name Patient
Patient und Arzt
2
Arztausweis
1
Arzt
3
4
5
6
7
Name Patient
8
Konnektor


1
Patient
CESUNDHEITSKARTE
2
Patient und Arzt
PIN korrekt?
[JA]
[NEIN]
5
Arztausweis
1
Arzt
4
6
3
7
8
Konnektor


Patient
Arzt
Datum
1
2
3
BROKER
4
5
6
7

Threats

ehc
3.6.08
1

(#Users ≈ 80 Mio)

T.USER

- Too authentication pieces will decrease security.
- Based on ~~of~~ non-integer data decision are take that ~~bad~~ negative consequences.
- Users can access external services without authentication, thereby importing malware.
- An insured might be pressed to give access to confidential data.
- Due to bad user friendliness of the systems ~~make~~, users make many errors which might lead to security breaks.
- Missing use of managable technologies may lead an urge to reveal confidential information by some groups (eg. handicapped).
- A service provider signs a manipulated document without knowing.

T. ADMIN (#Admins ≈ ?2000 central
+ ≈200000 decentral)

- Loss of development know-how due to personal change.
- Access to data ~~in the~~ belonging to an insured are not audited.
- Audit entries are changed or deleted, intentionally or unintentionally.
- Data protection violations by unsuitable storage place, unsuitable transport, unsuitable destruction, unauthorized copies.
- Wrongly configured components or services enable an attack.
- Usage of unauthorized components ...
- In case of security incidents, ~~this~~ may enable attacks or data protection violations.
- security violation are enabled because of too low awareness.
- security relevant process are not sufficiently defined. ... → attacks.
- Insufficient or missing definition of responsibilities lead to unauthorized actions and other attacks.
- By unauthorized connection of diverse datas, profiles may be made or confidentiality may be broken.

T. ATTACK

(# attacks unknown but probably small)

ehc
4.6.08
1

- unsuitable use of PINs & Password
  an attacker can get unauthorized access
- confidential and necessary data
  ~~are read by an att~~
  are read, changed or deleted
- telematic-relevant are created
- confidential person-related data
  is read intentionally or unintentionally
- attacker can use weaknesses in software
  to insert malware
- a health card is lost or stolen,
  an unauthorized person uses it,
  sniffs ~~spoofs~~ data of the owner,
  lets himself treat using that card.

T. HWSW (Hardware, Software)

≈ 200000
+ 80 Mio

- software contains non-allowed extra functionalities.
- a technical component does not work due to an "elementary event"
- due to bad contingency planning and a contingency data get to a less secure environment.
- a technical failure leads to changes in the data so that signed data is not valid anymore.
- stored data lost due to failure of the storage medium, unsuitable backup, external physical action or a general IT-threats.
- PKI services are not available. Thus some verification cannot be done and so attacks are possible.
- unforseen innovation in cryptanalysis may imply ~~may make~~ the exchange of all cards.
- the probative force (in the view of the court) of electronic signatures are weakend precedence cases

Summary

- Sovereignity of the insured.
  - → decide which data is stored
  - → right to read it.
  - ~~→ means to manage reading rights, ...~~
- ~~Retain~~ administration sovereignity of the insured
  - → means to manage access rights.
- Data protection
  - → physical access control (to elements in the telematic infrastructure)
  - → access control to software
  - → rights management
  - → person related data [confidentiality, integrity, authenticy, authorization]
  - → auditing (revisionable, non-repudiable)
  - → rights management of person related data which are processed on command.
  - → . protect against random damage
    . availability
  - → data seperation
- Basic IT-protection.

Security strategy

ehc
4.8.08
(4)

Corner points

- overall security concept
- protection of data and access
  - 2 card principle: electronic health card + doctor's card (or similar)
  - protection of data in the structure by crypto algorithms of strength at least high
  - encryption with individual keys (one for each insured)
- limitation of damages
  - data avoidance, data thrift, data seperation
  - seperation of the architecture into several security zones with evaluated components and services for security critical functions
  - proactive processes for fast reaction
- protection of participants (⇒ relationship between doctor and patient, mutual trust, MUST not be disturbed)

C2 - Schutzbedarfsdarstellung[26]

Zu näheren Infomationen zu den Informationsobjekten siehe C4.1

C2.1 - Io001 – Versichertendaten (data of the insured)

Typ des Schutzobjektes: Informationsobjekt		ID: Io001
Grundwert (basic criterion)	**Schutzbedarf** (Protection need)	**Begründung** (Reason)
Vertraulichkeit (confidentiality)	❒ niedrig (low) ✓ mittel (medium) ❒ hoch (high) ❒ sehr hoch (very high)	Die Versichertendaten sind personenbezogene Daten: Die darauf zugreifenden Akteure der TI (Arzt, Krankenkasse usw.) haben die für personenbezogene Daten übliche Vertraulichkeit einzuhalten (mittel).
Integrität (integrity)	❒ niedrig ❒ mittel ✓ hoch ❒ sehr hoch	Die Anforderungen an die Integrität von personenbezogenen Versichertendaten sind mit hoch einzustufen, da Manipulationen verhindert werden müssen. (z. B. Veränderung des Namens des Versicherten und somit erfolgt eine fehlerhafte Zuordnung), um die fehlerfreie Nutzbarkeit der gespeicherten Daten sicherzustellen.
Verfügbarkeit (1) (availability)	❒ niedrig ❒ mittel ✓ hoch ❒ sehr hoch	Könnte als mittel eingestuft werden, weil ggf. ein Leistungserbringer trotzdem den Versicherten behandeln könnte (per Unterschrift verpflichten zur Nachreichung der Daten, Barzahlung). Darüber hinaus besteht in Notfällen die Pflicht zur Hilfeleistung. Allerdings sind zu lange oder häufige Ausfälle der TI oder einzelnen Dienste für die meisten Abläufe stark akzeptanzmindernd. Daher wird ein hoher Schutzbedarf festgelegt.
Authentizität (authenticity)	❒ niedrig ❒ mittel ✓ hoch ❒ sehr hoch	Der Erzeuger (bzw. Übermittler) von Versichertendaten muss zuordenbar sein. Ein Verlust der Authentizität (Fälschung von Dokumenten) kann erhebliche negative Auswirkungen (Imageschäden, Akzeptanz eGK, ...) haben, nicht authentische Versichertendaten dürfen in der TI nicht benutzt werden. Eine Aussage über die Authentizität der Daten auf dem Wege bis zum VSDD wird dadurch nicht getroffen.
Nichtabstreitbarkeit (non-repudiation)	❒ niedrig ❒ mittel ✓ hoch ❒ sehr hoch	Ein Abstreiten der Erzeugung konkreter Versichertendaten, die im Rahmen eines Prozesses auf einer eGK oder über den VSDD verfügbar gemacht werden, darf durch den Erzeuger nicht möglich sein

[26] Einige Informationsobjekte sind nicht mehr aktuell und wurden daher gelöscht. Daher kann es zu fehlenden Nummern, wie z. B. C2.30 kommen.

chc
10.6.08
1

Details: Overall security concept

→ based and mentioned in the corr. law.

→ analysis of protection needs

→ protection goals
  ↳ decision on design
  ↳ minimize risks

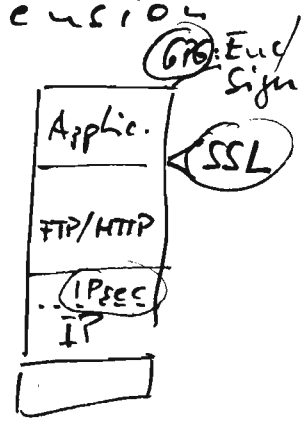
→ minimal requirements for
  security relevant processes,
  roles,
  responsibilities.

→ timely updates

consequences

- protection profiles, security concepts
  and security profile
  for every service and every components.

- realization of requirements and corner points
  → reduce amount of possible damage
  before reducing probability of damage.
  ⇝ to do so the architecture shall be distributed
  or split in several dimension
  e.g. OSI layers



  and tiers in
  (staged) security zone

- yearly update of the overally minimal standard

→ security management process

Also data storage shall be distributed.

Details: protection of data in the telematic infrastructure

- mechanism of strength "high"
  - MUST be supplied and defined by the structure
  - MUST follow the catalogue of algorithms given by gematik

Details: insured individual encryption

- ~~the~~ only the insured may decide about generation and use of his data

crypto concept

Details: data ~~the~~ shift and seperation

- no profile can be made
- use anymization or pseudonymization.

Details: separation of the architecture into security zones

according to:
- the owner of processes and data
- the classification and sensitivity of present data
- the users authorized to access the data
- the threat from the risk analysis

in particular the OSI-layers are used here.

Details: proactive processes for fast reaction

- fast reaction
- with tested contingency measures and plans
- time for recognizing an attack plus the reaction to it should be smaller than the time for a successful attack

* Reaction:
  fix maximal reaction times
  → CERT ~~teams~~
  \ Computer Emergency Responce Team

* Discover:
  fix maximal discovering time
  → Intrusion Detection System

* Prevent
  → use Security Patches

ehc
17.6.08
3

Details: Protection of the participants in the infrastructure

Basis: health information must stay secret to support trust between doctor and patient.

Cornerstone:

Every participant MUST that the law's definition are technically enforced by the infrastructure.

→ prevent unauthorized accesses (crypto)

→ analyze — " — afterwards (audit)

Protection goals

dic
17.6.08
4

- availability (... ✓)
- confidentiality (→ encryption ... crypto concept
  → authentication
  → auditing
  → key management)
- integrity
- authenticity
- non-repudiation of data transmission
- authorization and access control
- revisability

Next wednesday (25 June) we go to Bochum altogether!

ehc
18.6.08
(1)

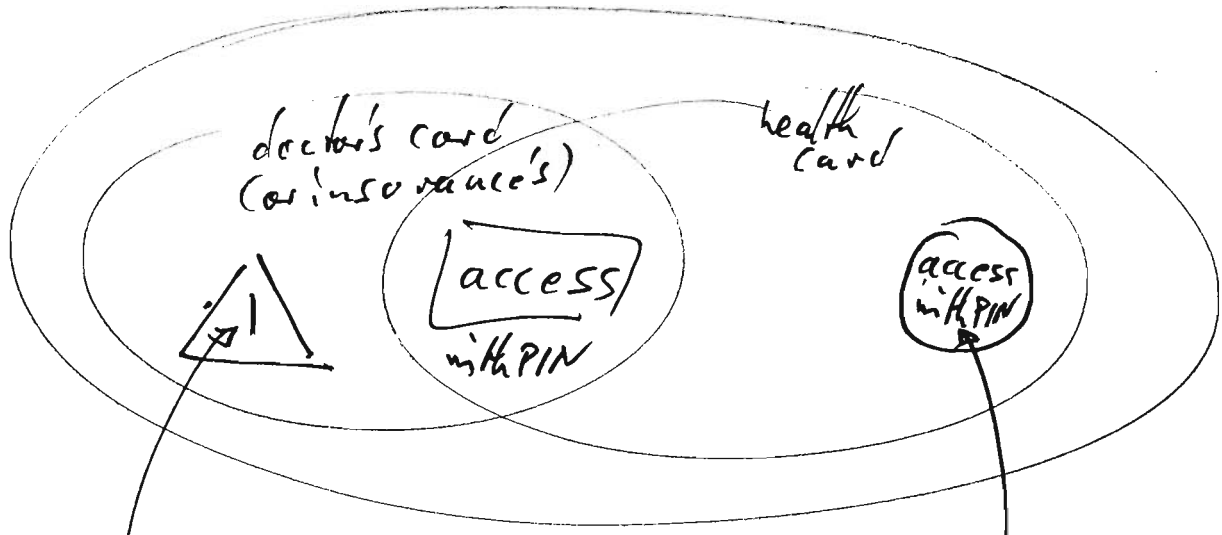
Overview over the structure

- decentralized components
  - computers at the doctors and health insurances...

- services
  - → patient folder (future)
  - → patient box
  - → ~~cent~~ emergency data

- ~~service relat~~ application related security services and rights management

Details: two card principle



access in emergency cases (under given rules to grant the insured person's rights)

access limited information (for example prescriptions)

- need secure authentication
  - doctor's card MUST be able to give 'qualified electronic signatures' refer to german law.

Consequences

- validity at the time of usage
  in particular, that procedure to revoke keys of lost or broke cards MUST be available.
- card management processes
- In cases where the insured's card/PIN is not available there MUST be a suitable, auditable technical procedure where acknowledgement and information of the patient is asked.

This leads to the

ROADMAP

release 0: • no online connection
• all data like · identification
· prescriptions
· emergency data

on card.

release 1: two card-principle in its strongest form.

- only an advanced electronic signature required
- use connector & card terminal
- networks must follow security requirements
- security infrastructure must follow policies
- services VSDM, VODM must follow minimal requirements for data protection and security. In particular, profiling impossible.

insured identity information

prescription data management

ehc
18.6.08
(3)

release 2: • to upload (or review) documents
the patient's card
needs be there anymore,
instead authorization
must have given.

'Appendix'

Cryptography concept

- description of used key materials
- description and minimal requirements of the life cycle of used key materials
- description, assumptions and minimal requirements of the ~~environ~~ environment.
- requirements on contingency plans
- definition for raising alarms.

Basis: TR 03116 by BSI
↑
this has ~~been~~ revised yearly

ehc
18.6.08
(4)

Migration- and release planning

TR : 6 years into the future

healthcard : 5 years
lifetime

---

time for
planning, specification,
testing, certification,
check and start } only 1 year

→ Many things are affected
by such updates.

---

problems with TR-03116.

- CV-authentication (Certificate Verification)
  - root ~~[illegible]~~ 2048 bit ~~RSA~~ key
  - so every card verifying a certificate chain needs ~~to~~ be able to perform 2048 bit RSA.

Yet: not all ~~[illegible]~~ authorized cards can do that

→ first only 1024 bit RSA is used.

- need hash function

  SHA1, RIPEMD160 till end 2009.

  SHA2 family till end 2013:

  so we SHA2 family.

  But health card spec only requires SHA1.

- technical difficulties with SHA2 family in connection with XML standards.

  XML standard: does not preview use of SHA2 family

  .NET: · use of SHA2 not yet defined

  · claim to have plans

  no reliable information.

  JAVA: not yet implemented fully.

- conflict of key length and hash algorithms for IPsec

  - all avaible VPN-concentrators use SHA1.
  - key length above 1024 bit may require exchange of hardware
  - the connector must SHA1 in the first and SHA256 later.

chc
18.6.08
6

- conflict with key length and hash fns in TLS (SSL-certificates,...)
  - available hardware security modules all use SHA1.
  - key length above 1024 bit for those hardware security modules are slow.

- missing procedures.

Diffie Hellman groups
- ~~are not~~ for IPsec are not defined in TR 03116.
- but the a gematik document requires DH groups 5 and 14 (see IPsec) from 2007 ... 2013 and EC groups optionally...

Hash function MD5
- used for DNSSEC but not allowed...

It is not planned to update DNSSEC in this framework.

RUHR-UNIVERSITÄT BOCHUM

iseb
E-Business
Security

Institut für Sicherheit im E-Business (ISEB)

Institute for E-Business Security

Links: eurobits | Horst Görtz Institut | a-i3 | Fakultät für Wirtschaftswissenschaft | L

Willkommen
Startseite
Profil
Arbeitsgruppen
Mitglieder

Aktivitäten
Unternehmen
Studierende

Veranstaltungen
ISEB-Workshop
XChange-Seminar

Publikationen
Arbeitsberichte
Aufsätze/Bücher
Dissertationen

Kontakt
Ansprechpartner
Impressum
Mailingliste

English

Herzlich Willkommen

ISEB-Workshop

Informationssicherheit im Gesundheitswesen

Einladung zum 6. ISEB-Workshop / 10. CCEC-Workshop
ANMELDUNG | ISEB-Workshop

Themen:

Datenschutz und Informationssicherheit in der Telematik-Infrastruktur des Gesundheitswesens
Sven Marx, Leiter Datenschutz und Informationssicherheit, gematik, Berlin

Der versichertenzentrierte Audit als Datenschutzfördernde Technologie der Gesundheitstelematik
Dr. Herbert Bunz, Associate Partner, Public Sector, S&C, Health Telematic Infrastructures, Security, Privacy, IBM, Stuttgart

Einführung der elektronischen Gesundheitskarte bei der DAK
Kai Lüssenhop / Harald Peetz, IT-Sicherheitsbeauftragte, DAK - Unternehmen Leben, Hamburg

Zeit: MI, 25.06.2008, 14.00 - 18.00 Uhr
Ort: Veranstaltungszentrum der Ruhr-Universität Bochum / Saal 3

gematik IBM DAK Unternehmen Leben

Anmeldung:
Hier gelangen Sie bis zum Anmeldeformular. Die Teilnahme ist dank der Unterstützung der Horst Görtz Stiftung entgeltfrei.

ISEB Workshop
Informationssicherheit Gesundheitswesen

25.06.08

Datenschutz und Informationssicherheit in der Telematik-Infrastruktur des Gesundheitswesens

SVEN MARX, gematik

Grundlage §291a/b SGB V

- → e Verordnung ~~(Pflicht)~~
- → e HIC
- → Versichertenstammdatendienst

} Pflicht

- → Notfalldaten
- → elektronischer Arztbrief
- → Patientenfach
- → Patientenquittung
- → Arzneimitteltherapiesicherheit
- → ePatientenakte

} freiwillig

270 KV
2200 Krankenhäuser
20000 Apotheken
195000 Ärzte/Zahnärzte
80 Mio Vers.
800000000 - 1000000000 Verordnungen

} Vernetzung

Gesetzliche Grundlagen

- Approbationsgebundenen Rechte
- Grundrechte auf informationelle Selbstbestimmung
- Rechteverwaltung durch den Versicherten
- Sicherstellungsauftrag der gematik

Entwurf?

§291a → Zugriffsregeln
→ ~~juristisch~~ versichertenzentriert
→ juristisch: Kopien der Behandlungsdokumente in der Hoheit des Versi.
→ Der Versicherte ist und bleibt Herr seiner Daten

Rolle der gematik

→ Gegründet 2005 aus §291b, Gesellschafter sind die 15 Spitzenverbände im alt. Gesundheitswesen

→ gematik ist nicht Betreiber, sondern spezifiziert ...

→ Ende 2008 ca. 130 intern 100 externe Mitarbeiter

→ Einvernehmen mit den Vertretern des Gesundheitswesens, BMG, BSI & BfDI

→ ... Interoperabilität, Kompatibilität und das notwendige Sicherheitsniveau

Umsetzung

ekiosk: wo?

Telematikinfrastruktur

eGK: 2 Schlüsselpaare (1 für Pflicht, 1 für freiwillig) ... Datenerhalt?

HBA: zusätzlich Unterschriftschlüssel

→ kein PIN frei eVerordnung schreiben lesen...

jetzt: 2048 bit / SHA2	ab 2011: EC

Anonymisierung?

Broker

Konnektor → verschlüsselte individuelle Verschlüsselung.

Fragen: Krypto-update? Migrationszeit: 12 Monate. Schlüsseltausch aller Komponenten möglich.

Patient ↔ Karte korrekt? Foto, VSD → Gültigkeit klar.

Datenerhalt? key recovery oder für Dritten mitverschlüsseln... (noch offen!)

25.06.08
(2)

Der versicherungszentrierte Audit als Datenschutz fördernde Technologie der Gesundheitstelematik

HERBERT BUNZ, IBM Stuttgart

- Datenschutz höchste Prio; Versicherten zustimmung
- neue Plattform für Informationsaustausch
- Einsichtsrechte, auch auf Audit-Infos (Wer hat wann was getan?) [mit meinen Daten]

Audit-Dienst

↳ erstellte Liste: Vertraulichkeit sehr hoch
(Einzelnachweis nur mittel)

Lösung von IBM

- WebApplication Server vs. XML Accelerator
- verschlüsselt abspeichern

⚠ Jeder Nicht-leistungserbringer macht sich strafbar wenn er auf medizinische Daten zugreift (die nicht seine eigen sind); selbst dann wenn der Betroffene zugestimmt hat. §307a

Einführung der elektronischen Gesundheitskarte bei der DAK

KAI LÜSSENHOP, HARALD PEETZ

25.06.08
(3)

- 2 RZ in Hamburg
- 13000 DV-Arbeitsplätze
- 300 TB Speicherkapazität...
- 300 Mitarbeiter im IT-Bereich.

~ Ausblick: Ausgründung der IT zur BITMARCK.

IT-Sicherheit

2 Beauftragte (Lü. & Pe.)

- Steuerung, Weiterentwicklung
- Definitionen
- Pläne
- ...
- Überprüfung Wirksamkeit
- Schutzbedarfsanalyse, Bedrohungs- und Risikoanalyse.
- Awareness-Maßnahmen.
- Auditing

~~Sicherheitsvorgaben~~:

- sicherer Betrieb der IT insgesamt — Nachweis!
- sichere PKI
- Sicherheitskonzept

RZ, Schutzziel sehr hoch

Zugang: Pförtner / Chipkarte / Vereinzelungsschleuse / Videoüberwachung / PINs / 3 Chipkarten / geteilte Passwörter / Protokolle

Rollenverteilung ~~Personal~~ → personeller Aufwand (8 Rollen → je ≥ 2 Pers. bei 24/7-Betrieb noch mehr!)

Tipps: Bewerben bei BITMARCK — Hamburg, München, Essen

www.bitmarck.de

On the ISEB workshop

ehc
1.07.08
(1)

- Why no biometrics?
  - → Doctors have best biometrics anyways.
- How to grant long life for the private key in case of loss of card?
  - → Cryptographically, two solutions are possible:
    - → key recovery
    - → encrypt for a third party

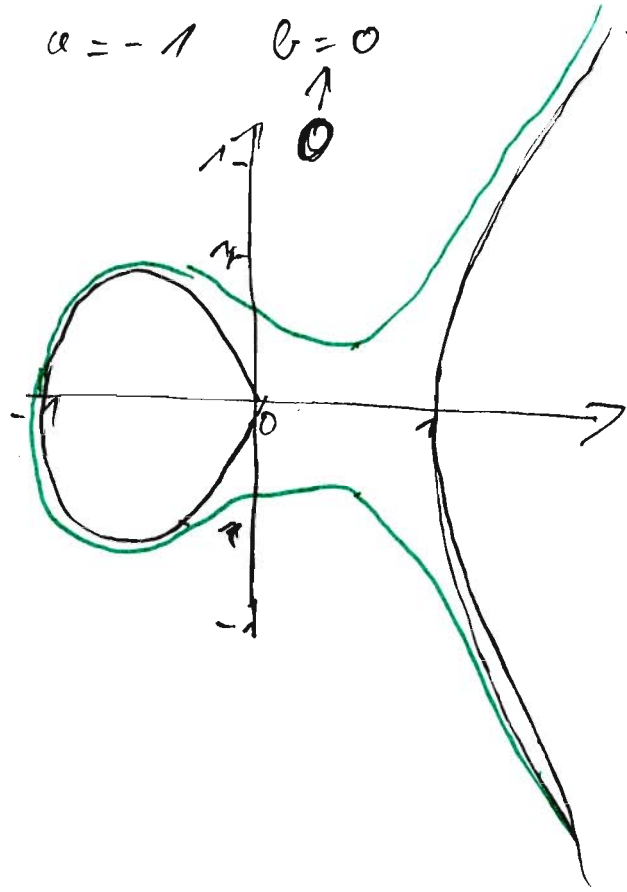
    Maybe add secret-splitting.
- Why should a hospital implement the voluntary services if only few people accept them?
  - → If one person dies because available information is not used, people will complain; even the hospital might be sued.
- Acceptance?
- gematik has no control/influence on the frontends.

Elliptic curves

$$E = \{ (x,y) \in \mathbb{F}^2 : y^2 = x^3 + ax + b \} \cup \{ \mathcal{O} \}$$

$a, b \in \mathbb{F} \quad 4a^3 + 27b^2 \neq 0$

$a = -1 \quad b = 0$

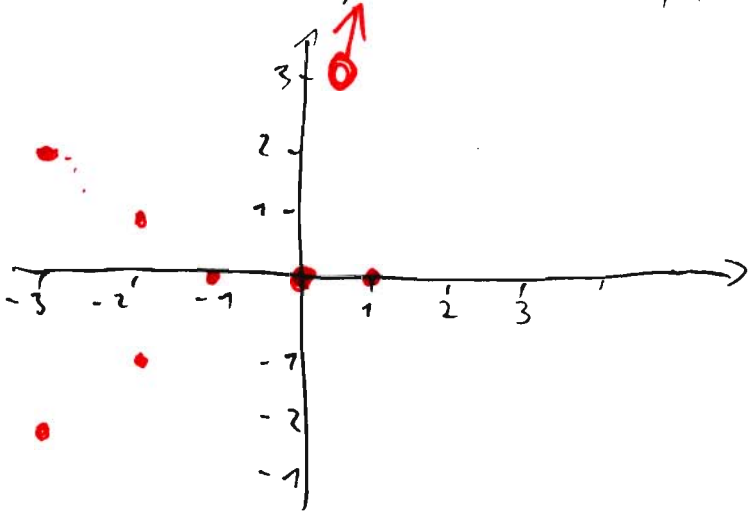


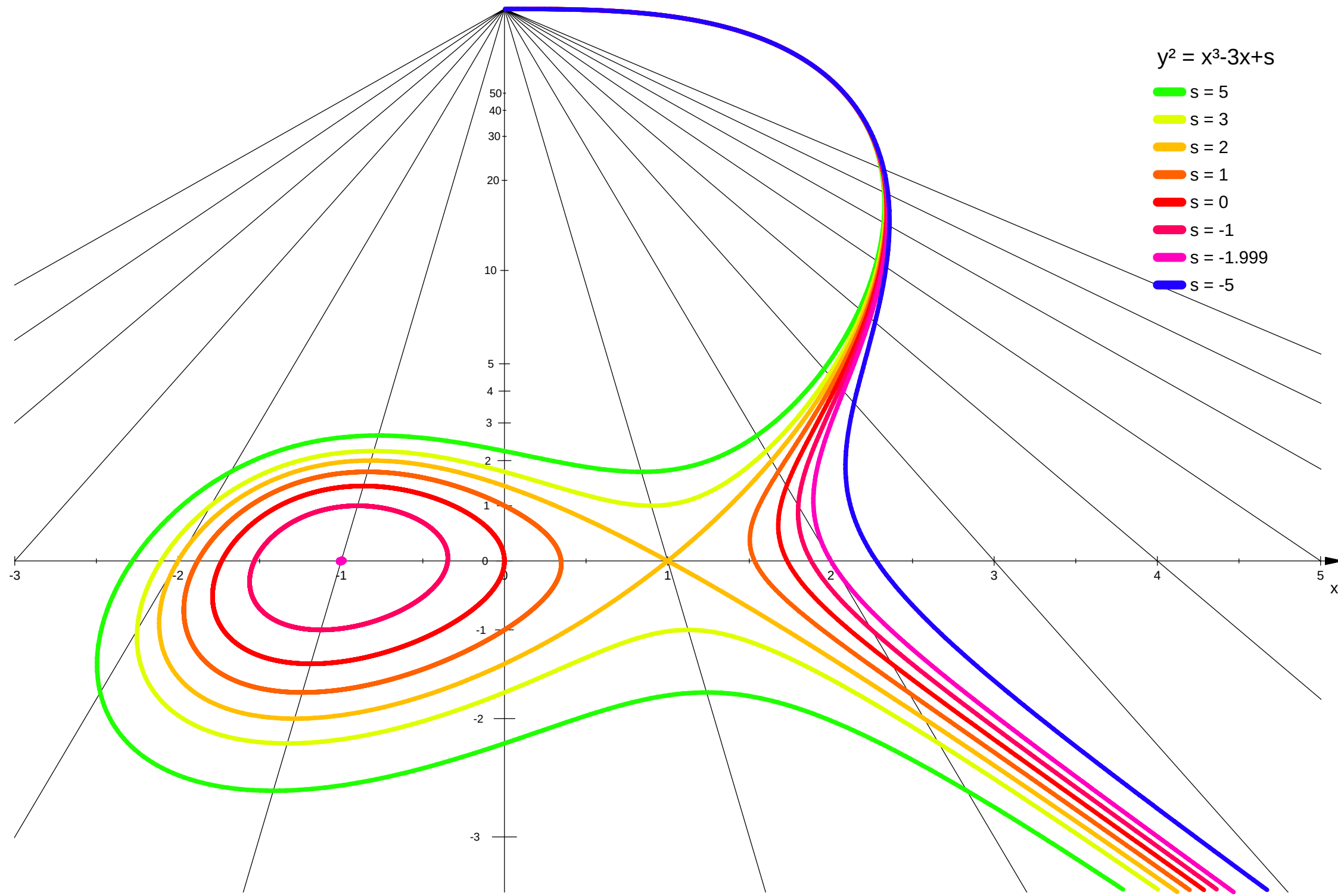
$$y^2 = x^3 - x$$
$$= x(x^2 - 1^2)$$
$$= x(x+1)\cdot(x-1)$$

$$y^2 = x^3 - x + \tfrac{1}{2}$$

$\mathbb{F}_7 \quad y^2 = x^3 - x$

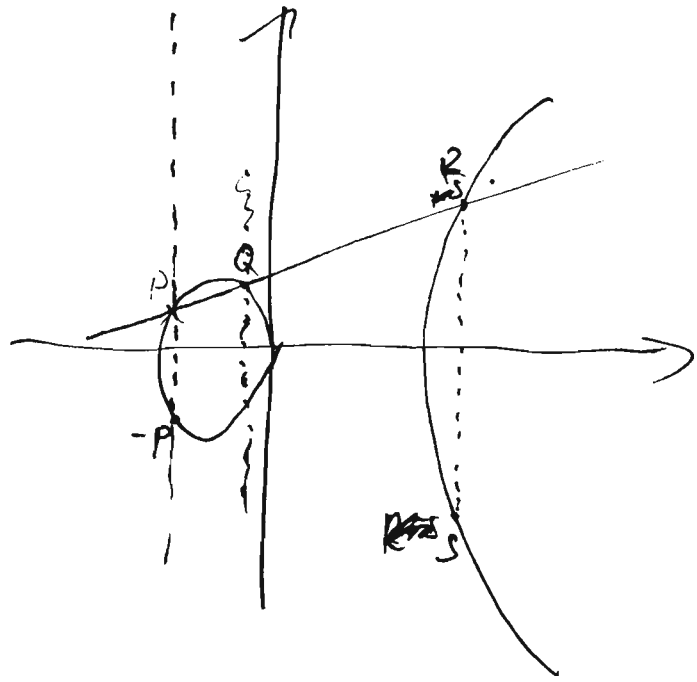
$(0,0), (1,0), (-3,2), (-3,-2), (-2,1), (-2,-1), (-1,0), \mathcal{O}$




y² = x³-3x+s
s = 5
s = 3
s = 2
s = 1
s = 0
s = -1
s = -1.999
s = -5
x
50
40
30
20
10
5
4
3
2
1
0
-1
-2
-3
-3
-2
-1
0
1
2
3
4
5

negativ $P = (x, y)$ $\quad -P = (x, -y)$

addition $-R = P + Q = S$



line: $t \mapsto P + t(Q-P)$

$$= \begin{pmatrix} x_P + t(x_Q - x_P) \\ y_P + t(y_Q - y_P) \end{pmatrix}$$

$$0 = -(y_P + t(y_Q - y_P))^2 + (x_P + t(x_Q - x_P))^3 + a(x_P + t(x_Q - x_P)) + b$$

$P = Q$ take the tangent

$Q = 0$ $\quad P + 0 = -(-P) = P$

$Q = -P$ $\quad P + (-P) = -0 = 0$

$P = (x_P, y_P)$ $\quad Q = (x_Q, y_Q)$ $\quad (x_P \neq x_Q)$

$P + Q = S = (x_S, y_S)$

$y = \alpha x + \beta$ (line equation)

$\alpha = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)$, $\beta = y_P - \alpha x_P$

ehc
2.07.
3

$S = (x_S, y_S)$

$\cancel{(-(\alpha x_S + \beta))^2 = x_S^3 + \overset{a}{\alpha} x_S + b}$

$(-(\alpha x_S + \beta))^2 = x_S^3 + a x_S + b$

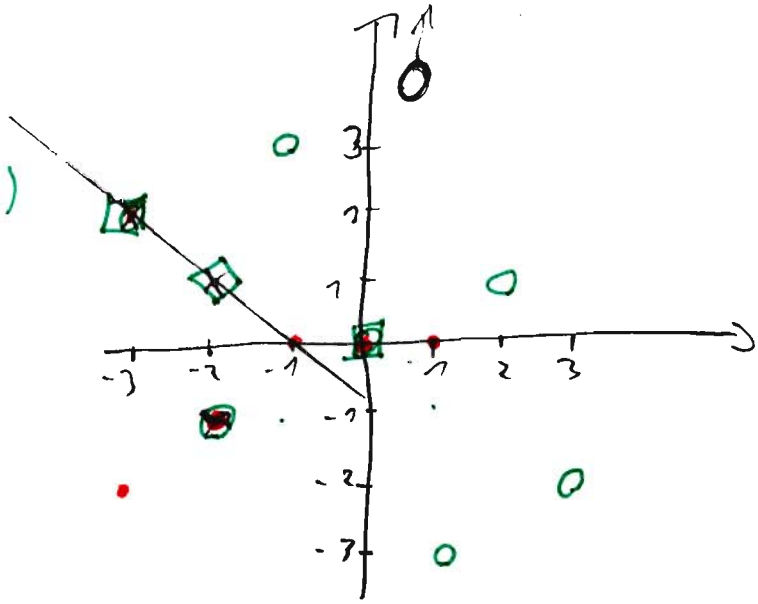
$$\boxed{x_S = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_Q - x_P, \quad y_S = -y_P + \frac{y_Q - y_P}{x_Q - x_P} \cdot (x_P - x_S)}$$

$x_P + x_Q + x_S = \alpha^2$

$y^2 = x^3 - x$ over $\mathbb{F}_7$

$(-3,2) + (-2,1)$

$(-3,2) + (0,0) = (-2,1)$



Size

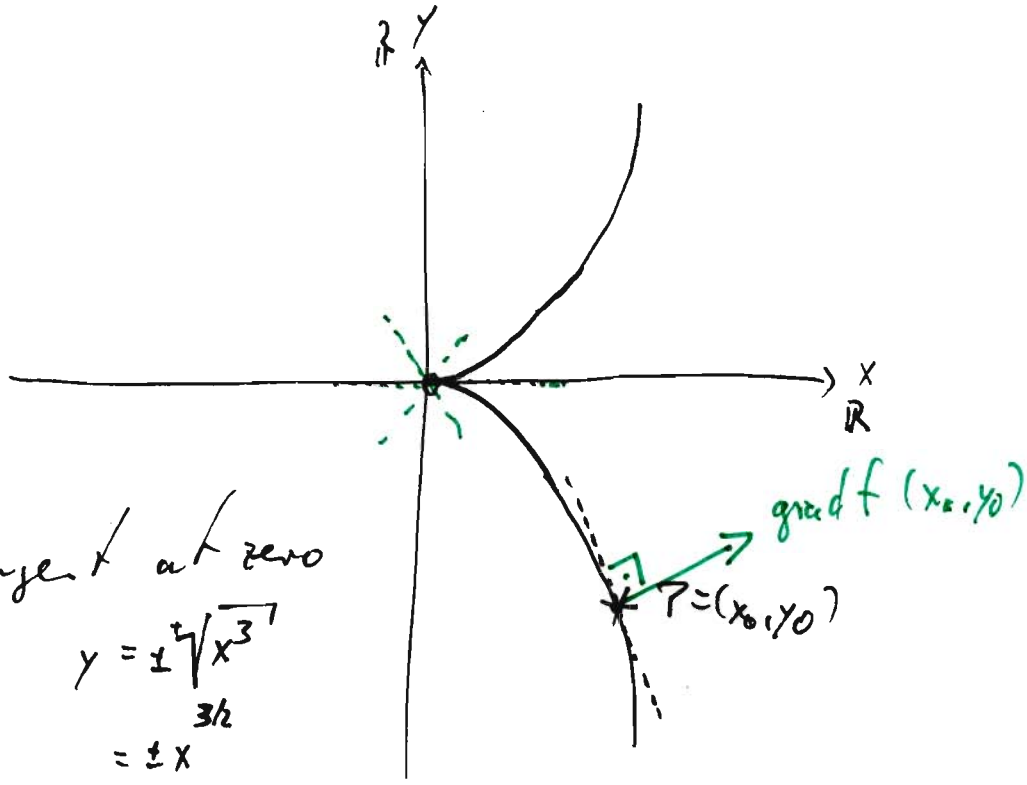
$\# E \leq 2q + 1$

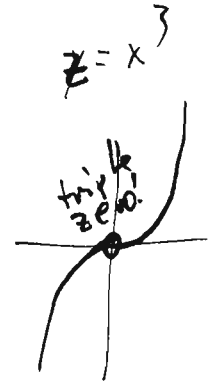
$y^2 = x^3 + ax + b$

$|\# E - (q+1)| \leq 2 \cdot \sqrt{q}$

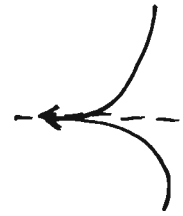
8.7.08
ehc
1

$E: \quad y^2 = x^3 \qquad$ so here $2^2 a^3 + 3^3 b^2 = 0$





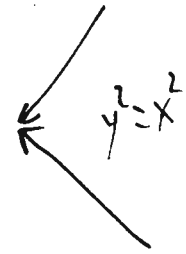
Tangent at zero to $y = \pm\sqrt[2]{x^3}$
$= \pm x^{3/2}$



$(0, 0; 0)$

$y' = \frac{dy}{dx} = \frac{3}{2} x^{1/2}$

$\rightsquigarrow$ "Double" tangent at $(0,0)$



$\rightsquigarrow$ NOT smooth (singular)

Give $E: f(x,y) = -y^2 + x^3 + ax + b =: f(x,y)$

What are the tangents? ... at some pt (x_0, y_0)?

$$\frac{\partial f}{\partial x} = 3x^2 + a$$

$$\frac{\partial f}{\partial y} = -2y$$

$$\boxed{(\text{grad } f)(x_0, y_0)} = \begin{bmatrix} \frac{\partial f}{\partial x}(x_0, y_0) \\ \frac{\partial f}{\partial y}(x_0, y_0) \end{bmatrix}$$

Tangent is anything orthogonal to the gradient and passing through the pt.

8.7.08
ehc
2

Def A point (x_0, y_0) of a curve $f=0$ is called smooth iff

$$(\operatorname{grad} f)(x_0, y_0) \neq 0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

A curve $f=0$ is <u>smooth</u> iff all its points are smooth.

When looking for a non-smooth point on a curve:

$$f(x_0, y_0) = 0$$

$$\frac{\partial f}{\partial x}(x_0, y_0) = 0$$

$$\frac{\partial f}{\partial y}(x_0, y_0) = 0$$

In our case:

$$\left.\begin{aligned} -y^2 + x^3 + ax + b &= 0 \\ 3x^2 + a &= 0 \\ -2y &= 0 \end{aligned}\right| \Rightarrow y = 0 \quad \text{in } \mathbb{F}^2 \ni (x_0, y_0)$$

that is exactly

$$\left.\begin{aligned} x^3 + ax + b &= 0 \\ 3x^2 + a &= 0 \end{aligned}\right\} \text{ in } \mathbb{F} \ni x_0$$

that is exactly x_0 must be a double zero of x^3+ax+b,

$$x^3 + ax + b = (x - x_0)^2 (x - x_3)$$

$$= x^3 - \underbrace{(2x_0 + x_3)}_{-x_0^2 x_3} x^2 + (x_0^2 + 2x_0 x_3) x$$

$\hookrightarrow$ $x_3 = -2x_0$, $a = -3x_0^2$, $b = +2x_0^3$.

$\hookrightarrow$ $4a^3 + 27b^2 = 0$.

The electronic health card & related issues:

The German ehc: Interface description of the card

Richard Tantius

Introduction

- Today: Part 1, specification of the electronic interface of the card.
  - Document: gematik_eGK_Spezifikation_Teil1_V2_2_0_3393
- Includes:
  1. basic commands
  2. basic required functions of the card operating system
  3. basic security features
  4. basic security algorithms
- The document describes how the card *behaves* at its interface
- and how the COS has to processes commands.
- It does not specify the structure of the Card Operating System (COS)
- Is supposed to be used as a basis for,
  - the command structure
  - Functions

  of an eHC conformant operating system.

Introduction

Target audience:

- addresses manufacturers of card operation systems (COS)
- application programmers who have to communicate with the card directly
- and students who want to know more details

Introduction keywords of the document

gematik_eGK_Spezifikation_Teil1_V2_2_0_3393:

- The document explicitly uses the precisely defined keywords from [RFC2119]:
  - MUSS — MUST
  - DARF NICHT — MUST NOT
  - SOLL — SHOULD
  - SOLL NICHT — SHOULD NOT
  - KANN — MAY
- The document has normative and informative chapters.

Introduction

- The document is build bottom up.
  - First details (artefacts) are explained, for example:
    - hash and crypto algorithms that are available on the card
    - how does the card communicate
  - Important details will be discussed
- Chapter 15 “Commands” shows the major context
  - Can be used for a top / down approach
  - Outer sight on the card
  - Defines commands:
    - ISO/IEC 7816 standard commands
    - how they have to be processed
  - In fact, only a very long list of commands provided by the card.

Introduction

- Commands are speared into the following groups (chapter 15 “Commands” subchapters)

1. Roll-Back / Roll-Forward
2. Management of the object system
3. Access to structured data
4. Access to data in transparent EF
5. Access to data objects
6. User verification
7. Component authentication
8. Kryptobox commands
9. Miscellaneous

Important artefacts

How does the card communicate with an external entity?

Communication

normative chapter (no. 12)

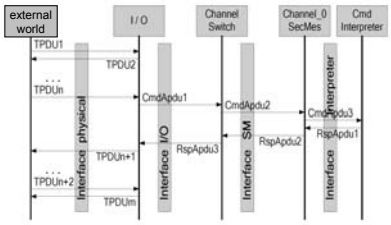
Request – Response

- Communication with an external entity through a channel in half-duplex
- Card acts as a server
  - Communicating entity sends messages (commands)
  - Card answers
- Communicating entity can only send a new commands, if the previous Message was accepted.

Communication

- Before communication can be started, the electrical interface has to be activated.
- The electrical interface can also be deactivated again
- Activation MUST and deactivation SHOULD to be done as described in ISO **7816-3**

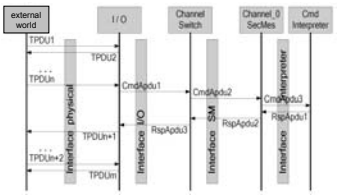
Communication



- Like in the OSI-Reference model there are layers
  - working on the processing of a command
- Commands are sent as command APDUs
  - (Application Data Unit)

Communication

- TPDU (Transport Protocol Data Unit)
  - Separates APDU into one or more TPDUs
  - Reassembling by the I / O unit.
- SecMes
  - Unpacks message if Secure Messaging was used.
  - Means that messages can be encrypted.
- Response APDU is sent back



Communication

Structure of the command ADPU:

CLA	INS	P1	P2	Data	Le
Header				Body	

- Class Byte (CLA): contains command class
- Instruction Byte (INS): code of the command
- CLA and INS precisely define the command that is supposed to be executed
- Parameters P1 and P2, are variables needed for the execution of a command
  - MUST be encoded in octets
- Data field: Is optional, contains octet string, with variable length from 1 to 65535.
- Le field tells how many octets are given in the data field

Communication

Structure of the response APDU:

- Data field: Is optional, contains octet string, with variable length from 1 to < length of the data field of the original command APDU
- Trailer: contains two octets, with status massages of the executed command

Important artefacts

The card is supposed to be secure, not everybody should be able to execute commands!

Access control

normative chapter (no. 11)

Almost all command are protected by access control rules.

- Access types and Access conditions form
- Access Rules
- Access evaluation: According to the Access rules the COS decides if a certain command is allow to be executed

Important artefacts

Object System

Objects and the Object System

normative chapter(s) (no. 9 and 10)

- The card is supposed to be a secured data storage
  - The card can save data like a hard disk
  - The access to files is controlled by access rules
    - COS makes sure those rules are obeyed
    - Often User verification is required
    - and Component authentication
    - Also a secure Data transfer is mostly enforced
  - Files (Objects) are hierarchically structured
  - The card provides an Object search

Objects and the object system

- Different objects are available:
  - The type of an object depends on the attributes it has
- For example a key material object, it says:
- 9.2.3.1 private RSA Key, G1 (normative)

  Is required to save the private part of an asymmetric RSA key pair. The specification of applications have take the following into account:
  - (N87) A privateRsaKey MUST have an attribute as describe in (N21)a
    - (N21)a (from Chapter 7 “security algorithms”): The COS MUST provide RSA keys with a length n chosen form the set {2048}
  - (N88) A privateRsaKey MUST have an attribute d, its value is an integer from the interval [1, n-1].

Objects and the object system

- 9.3.1 Folders
  - Folders are needed to provide a hierarchical arrangement of Objects in an object system. In this document a folder is a super type of:
    - Application (9.3.1.1)
    - Dedicated Files (9.3.1.2)
    - Application Dedicated Files (9.3.1.3)
  - According to [7816-4] the following rules have to be applied when specifying an application:
    - (N98) A Folder MUST have exactly one attribute of the type lifeCycleStatus (9.1.3 ↓)
      - [...] (N71) The value of lifeCycleStatus MUST be an Element form the following set {„Operational state (activated)“, „Operational state (deactivated)“} [...]
    - (N99) A Folder MUST have exactly one attribute of the type accessRuleList (9.1.4)

Objects and the object system

- (N100) A Folder MUST have a maybe empty list of children, with child objects
  - a) The COS MUST, taking the maximum nesting depth into account, support list elements of the following object types *(not included in Applications):*
    - » Dedicated File (9.3.1.2)
    - » Application Dedicated File (9.3.1.3)
    - » File (9.3.2)
    - » Password (9.4)
    - » Symmetric Authentication object (9.5.1)
    - » Private Key Object (9.5.2)
  - b) The COS MAY include other object types on the list
    The COS MAY deny other object types on the list

Objects and the object system

- Other important objects are provided
  - For Example:
    - (9.3.2.1) Transparent Elementary File
      - Stores data in a body attribute
    - (9.4) Password
      - Stores the user Secret

Commands: Overview

1. **Roll-Back / Roll-Forward**
2. Management of the Object System
3. Access to structured data
4. Access to data in transparent EF
5. Access to data objects
6. User verification
7. Component authentication
8. Kryptobox commands
9. Miscellaneous

ehc
3
8.07.

Aim: cant calculate discret log

Size of E is an n-bit prime

we need $2^{n/2}$ ~~operations~~ operations

size of EC is at least 160 bit ~~for prime p~~

~~Factorisation~~

The size of the largest primefactor should be at least 160 bit.

Technical Requirements

- p shall be congruent 3 mod 4
  $\Rightarrow$ efficient point compression

- $A = -3 \bmod p$
  $\Rightarrow$ arithmetical advantages

- To avoid overflows we require $\#E_{\mathbb{F}_q} < q$

Security Requirement

- The curves are not one curves.
  $\#E_{\mathbb{F}_p} \neq p$

- The group order should be prime to counter small-group attacks
- Verifiably pseudo-random.

lec
4
8.03.

ElGamal Encryption with EC

Encryption

Input: Massage X, public key A, setup (E, P)

choose $\tau \in_R E$

compute τP in E

compute $\tau A + X$ in E

return $(\underset{T}{\underset{\shortparallel}{\tau P}}, \underset{Y}{\underset{\shortparallel}{\tau A + X}})$

Output (T, Y)

Problem:

Form of the massage

Decryption

Input: ciphertext (T, Y), private key α, setup $A = \alpha P$

$$X = Y - \alpha T$$

Output: Plaintext X

The German electronic health card: Interface description of the card.

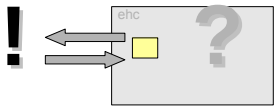
Part 2: Commands

Richard Tantius

Commands

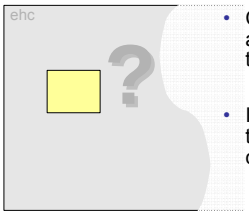
Commands (with related internals):

- miscellaneous commands:
  - Example from the command group "user verification": verify
- Cryptoboxcommands:
  - PSO Compute Digital Signature
  - PSO Decipher
  - PSO Encipher
  - PSO Hash
  - PSO Transcipher
  - PSO Verify Certificate



Verify

Command description

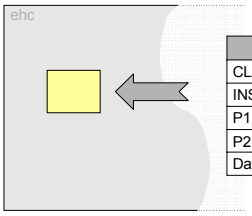


- Compares the attribute secret of a password object with data in the commandAPDU
- If successfully performed, then the security state of the card is changed

Verify

Input

What is passed to this command(?):

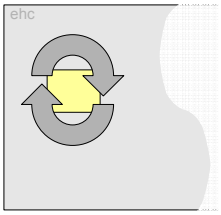


	Contents	Description
CLA	00	CLA Byte [7816-4]
INS	20	Instruction Byte [7816-4]
P1	00	Data contains verification data
P2	XX	passwordReference
Data	XX..YY	verification Data

Verify

Internal resources

What internal resources does this command use(?):

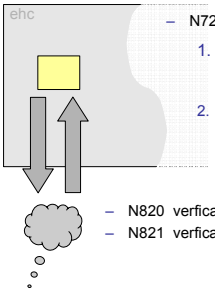


- Internal functions used:
  - searchPwd
  - AccessRuleEvaluation
  - clearPasswordStatus
  - setPasswordStatus
- Used data on the card
  - there is an: affectedObject
    - Password Object
  - affectedObject.secret
  - affectedObject.retryCounter
  - affectedObject.transportStatus

Verify

Use Case: Compare user secret

- N819 passwordReference is the reference to the affected password and must be chosen as described in :
  - N728 p.R. consists of two components:
    1. location codes:
       = 00 → it is a global Password Object
       = 80 → Dedicated File (DF) specific Password
    2. Identifier
       - identifies the affected Password Object
         (The PW-Obj. MUST be chosen according to N150)
       - MUST be encoded as:
         passwordReference = location + identifier
  - N820 verficationData contains the user Secret
  - N821 verficationData MUST be encoded as in N81



Verify

Security features:

- PW-Obj, has different attributes:
  - pin (the actual password)
  - minimumLength ([4,12])
  - retryCounter
  - PUK (pin)

according to the common security concept of counting wrong password attempts and denying access when the counter exceeds a certain limit.

- PIN Attribute in PW-Object and DF
  - encrytion does not seem to be required
  - digits [0, ..., 9]

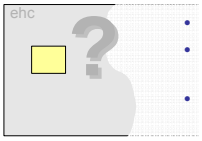
hash function is not applicable because average password length to short?

Crytoboxcommands

- PSO Compute Digital Signature
- PSO Decipher
- PSO Encipher
- PSO Hash
- PSO Transcipher
- PSO Verify Certificate

PSO Compute Digital Signature

Command description



- Signs data via a private key
- Private key and used algorithm are chosen with MSE-Command
- Data that is supposed to be signed is included in a parameter

- MSE-Command?
  - MANAGE SECURITY ENVIRONMENT
  - Changes seIdentifier in current folder and in channelContext Objects Elements of the keyReferenceList

available keys in current security level

PSO Compute Digital Signature

Input: What is passed to this command(?)

contents description

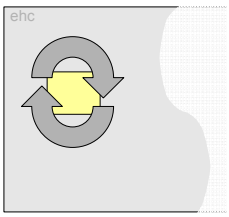
	Inhalt	Beschreibung
CLA	'00'	CLA Byte gemäß [7816–4]
INS	'2A'	Instruction Byte gemäß [7816–4]
P1	'9E'	Beschreibung der Antwortdaten, hier digitale Signature
P2	'9A'	Beschreibung der Kommandodaten, hier „zu signierende Daten"
Data	'XX...YY'	dataToBeSigned
Ne	length	Anzahl der erwarteten Oktette in den Antwortdaten

- P1 description of the data the answer contains, in this case: a digital signature
- P2 description of the command data, in this case: data that is supposed to be signed

PSO Compute Digital Signature

Internal resources

What internal resources does this command use(?):

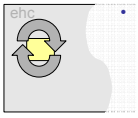


- Internal Functions used:
  - SearchSecretKey
  - AccessRuleEvaluation
  - Internal signing functions:
    - RSA_ISO9796_2_DS2_SIGN
    - RSASSA_PCKS1_V1_5_SIGN
    - RSASSA_PSS_SIGN
    - ELC_SIG

PSO Compute Digital Signature

Internal resources

What internal resources does this command use(?):

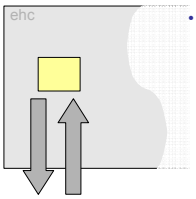


- Used Data on the card
  - affectedObject
    - a Secret Key Object
  - affectedObject.keyAvailable
  - channelContext Object (needed to find Key)
    - channelContext.keyReferenceList. signatureCreation.keyReference
    - channelContext.keyReferenceList. signatureCreation.algID

- What is a channelContext Object (chapter13!)?
  - combines Channel [7816–4] specific attributes
  - values depend on the „Security Environment" (MSE) of a channel

PSO Compute Digital Signature

Use Case: Signing the data field



- N873 dataToBeSigned: contains the data that is supposed to be signed.
  - (it's length depends on algId)

When algId (depends on *SE*) equals:

a) rsaClientAuthication
b) signPKCS1_V1_5
c) signPSS
d) sign

} Results in different ammounts of Octets for dataToBeSigned

- N874 length ← length of the expected answer data
  (– MUST be chosen form a specific Interval ...)
- N875 a certain APDU MUST be used ...

sign9796_2_DS2 alg. has separate Use Case ...

PSO Compute Digital Signature

Internal command processing:

- N882 COS MUST be support as described in the use case ...
- N883 when channelContext.keyReferenceList.signatureCreation
- is empty → MUST terminate with Trailer NoKeyReference
- is not empty →
  affectedObject = SearchSecretKey(currentFolder,
  channelContext.key.ReferenceList.signatureCreation.keyReference
  channelContext.keyReferenceList.signatureCreation.algID)
- keyNotFound (MUST)→ trailer: KeyNotFound
- notSupported (MUST)→ trailer: UnsupportedFunction
- N884 AccessRuleEvaluation(affectedObject, CLA, INS, P1, P2)
- N885 ...
- N886 The Signature is computed as shown
  ...

(on the next page)

PSO Compute Digital Signature

Internal command processing:

- N886 The Signature is computed as shown below:

a) sing9796_2_DS2 ...
b) signPKCS1_V1_5
signature = RSASSA_PCKS1_V1_5_SIGN(
affectedObject.privateRsaKey,
dataToBeSigned
)
c) rsaClientAuthentication or signPSS
signature = RSASSA_PSS_SIGN(
affectedObject.privateRsaKey,
dataToBeSigned
)
d) signECDSA
signature = *R* || *S*, mit
(*R*, *S*) = ELC_SIG(*affectedObject.privateElcKey*, *dataToBeSigned*)

PSO Compute Digital Signature

RSA, ISO9796–2, DS1, SIGN

Input:	digestInfo	arbitrarily chosen oktettstring used as „Digest Info“
	PrK	private RSA Key Object (9.2.3)
Output:	S	Oktettstring, representing the Signatur
Errors:	–	DigestInfoTooLong

Notation: *S* = RSASSA_PCKS1_V1_5_SIGN(*PrK, digestInfo*)

PSO Compute Digital Signature

The COS MUST perform the following Aktions, including the definitions:
n = *PrK.n*, *d* = *PrK.d*.

a. Step 0: If OctetLength(*digestInfo*) > 0,4 OctetLength(*n*), then stop with error: DigestInfoTooLong.
b. Step 1: Set *EM* ← ´00´ || *digestInfo*.
c. Step 2: Set *EM* ← ´FF´ || *EM*.
d. Step 3: If OctetLength(*EM*) < OctetLength(*n*) – 2, then goto Step 2
e. Step 4: Set *EM* ← ´01´ || *EM*.
f. Step 5: Set *m* ← OS2I(*EM*).
g. Step 6: Set *s* ← m^d mod *n*.
h. Step 7: Set *S* ← I2OS(*s*, OctetLength(*n*)).

PSO Compute Digital Signature

ELC

Input:	H	arbitrarily chosen oktettstring representing a Hashvalue
	PrK	ein privater ELC Key (Object)
Output:	R	Oktettstring, fist Part of the ECDSA Signatur
	S	Oktettstring, second Part of the ECDSA Signatur
Errors:	–	–

Notation: (*R*, *S*) = ELC_SIG(*PrK, H*)

PSO Compute Digital Signature

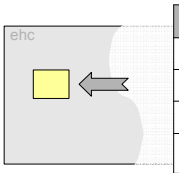
The COS MUST perform the following Aktions, including the definitions:
n = *PrK.domainParameter.n*, *G* = *PrK.domainParameter.G*,
dA = *PrK.domainParameter.d*, *L* = *PrK.domainParameter.L*

a. Step 1: k ← RNG({1,2, …, n – 1}).
b. Step 2: Q ← [k] G mit $Q = (x_Q, y_Q)$.
c. Step 3: r ← OS2I(FE2OS(x_Q)) mod n.
If r *equals* null, then go to Setp 1.
d. Step 4: k_{inv} ← k^{-1} mod n.
e. Step 5: s ← k_{inv} ($r\, d_A$ + OS2I(H)) mod n.
If s *equals* null, then goto Step 1.
f. Step 6: R ← I2OS(r, L).
S ← I2OS(s, L).

PSO Encipher

Input

What is passed to this command(?):



enciphered text

	contents	description
CLA	00	CLA Byte
INS	2A	Instruction Byte
P1	86	Description of the answer data
P2	80	Description of the command data: here plaintext
Data	XX...YY	plain
Ne	length	amount of expected octets in the answer.

Encipher during command processing

N917

- The commandMessage is split:

a) plain = algDO || plainDO
b) algDO = '80 01 algID'

Encipher during command processing

N918

- The cipher is computed as followed:
  - If algID has the value: elcSharedSecretCalculation
    i. plainDO = 'A0 - L_{A0}- (oidDO || keyDO || mDO).
    ii. oidDO = '06- L_{06} – oid'
    iii. keyDO = '7F49 - L_{7F49} - (86 – L86 – PO_B)'
    iv. mDO = '80 - L_{80} – M'
    v. ...

    ...

PSO Encipher

Finall output:

data	contents	description
XX..YY	chipher	chipher text

trailer	contents	description
90 00	NoError	successful encipher operation

Introduction

It is very important that private data like those on the electronic health card from a patient is secure also against attackers that have the opportunity to physically penetrate the Smartcard with special equipment to get the private data.
The scope of this lecture is to give a brief introduction in the specification of a Smartcard according to ISO 7816 and summarize the possible attacks on it.

What is a Smartcard?

Briefly a Smartcard can be described as a "Computer-on-a-Chip". All components from the von Neumann architecture can be found on a Smartcard more precisely on the Chip from a Smartcard (see fig. 1 and fig. 2).

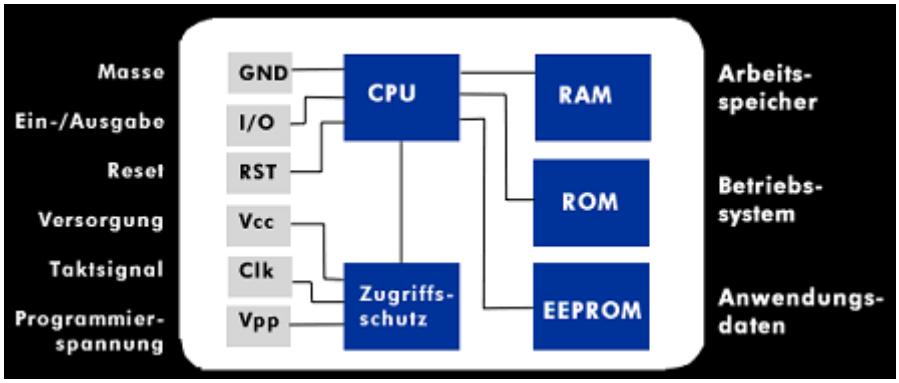


Figure 1: Components of a Smartcard.

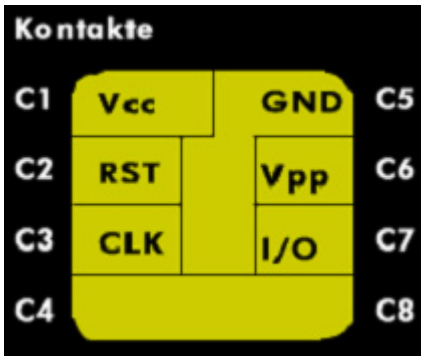


Figure 2: Contacts from the Chip.

A Smartcard has to be interoperable. This means that a terminal (technically called CAD – Card Accepting Device) can read different Smartcards with different applications. This is regulated by the ISO (International Organization for Standardization). The standard of interest for us is ISO 7816. In this standard three Smartcard sizes are defined. The eGK (electronic health card) has to be ID-1 which is also the most common Smartcard size.
Not only is the shape of a Smartcard, also the communication between the CAD and the Smartcard is defined in the standard.

Possible security vulnerabilities and protection against these

First we have to define who can be the hacker. In our eGK- World we have several participants. Namely:

1.) The Smartcard vendor (Hardware)
2.) The Smartcard vendor (Software)
3.) The Smartcard owner, namely the patient
4.) A thief, which obtain a Smartcard.
5.) The doctor
6.) The CAD (Card-Terminal)

All this actors open up security vulnerabilities or are possible attackers. Even the owner could have the interest in manipulating his data on his Smartcard. We assume that we are powerless against backdoors or other none-public knowledge from the Hardware and Software vendors to read out private data from the Smartcard.

After we defined who can attack we show briefly how to attack. Attacks differ whether they are done passively (non-invasive) or active (invasive attacks).

First let us discuss about invasive attacks:

1.) Layout Reconstruction
2.) Manual Microprobing
3.) Memory read out
4.) Particle Beam

Now the non-invasive attacks:

1.) Power Break
2.) Glitching
3.) Random Seed
4.) Timing
5.) Differntial Fault Analysis
6.) Single Power Analysis

Conclusion

We learnt several vulnerabilities in the Smartcard technology. Beside the possible attacks the hacker has to make a trade-off between his gain from the private data and his costs to get this data. Only limited groups can afford the knowledge and the Hard- Software to hack a Smartcard. The conclusion is, if the tests for the Hard- and Software made properly the security from an eGK is at a very high point.

ehc 15.7.08 Sien Mece

ehc hardware — smartcard

→ ISO 7816. http://en.wikipedia.org/wiki/ISO_7816

Invasive attacks

- Layout reconstruction
  ⌜Use a strong acid to resolve all but the silicon. Look with a microscope... ⌟
- Manual microprobing
  ⌜Reattach chip contacts, use electron microscope to see details... ⌟
- Memory read out
- Particle beam
  ⌜Burn nm holes and replace with other contacts ... ⌟
- Reattach test contacts
  ⌜Vendors use additional contacts for testing. These are disconnected at special fuses before delivery. The attackers can reattach these... ⌟

Non-invasive attacks

- power break
  ⌜A short power break may lead to important info, like an unregistered answer to a PIN check... ⌟
- glitching
  ⌜Manipulate... e.g. clock, temperature, ... to force malfunctions... ⌟

- ~~Random Seed~~
- Differential Fault Analysis
  [Induce an error and study the difference to a valid computation]

- Single Power Analysis, Differential Power Analysis
  [Example: Square & Multiply
  Countermeasures:
  - Use dummy operations
  - Use noise
  ]

- Random Seed Attack
  ...?

- Timing Attack
  [Most simple power analysis.]

Physical countermeasures

Thursday 19.00
James Joyce