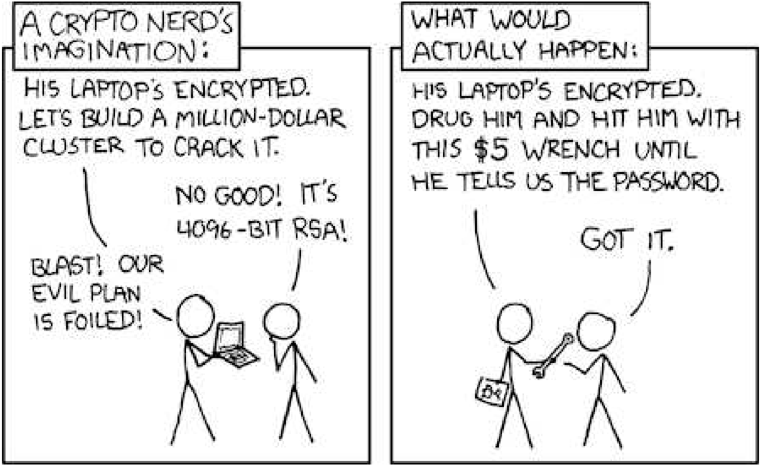
Cryptanalytic world records, summer 2014

Brute force cryptanalysis

Dr. Daniel Loebenberger



Source: `http://xkcd.com/538/`

Overview

Dictionary attacks

Exhaustive key search

Collision finding

Overview

Dictionary attacks

Exhaustive key search

Collision finding

File /etc/passwd:

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
...
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
...
daniel:x:500:500::/home/daniel:/bin/bash
```

File /etc/shadow:

```
root:$1$CQoPk7Zh$370xDLmeGD9m4aF/ciIlC.:14425:0:99999:7:::
bin:*:14425:0:99999:7:::
...
rpm:!!:14425:0:99999:7:::
...
daniel:$1$wKAP1RyH$JeCAcEGhSGVlD0J7.AMg.0:14396:2:5:7:30::
```

Details on the encrypted password:

`> man 3 crypt`.

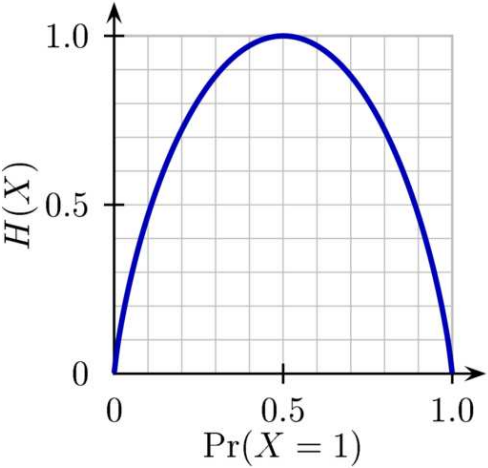
John the Ripper (`http://www.openwall.com/john/`) provides by default a list of 3546 most frequently used passwords:

```
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
carmen
mickey
...
```

Claude Shannon (1951):

> *"The entropy is a statistical parameter which measures in a certain sense, how much information is produced on the average for each letter of a text in the language. If the language is translated into binary digits (0 or 1) in the most efficient way, the entropy H is the average number of binary digits required per letter of the original language."*

Binary entropy:



We have the following table of the entropy per symbol for uniformly selected passwords:

Alphabet	Cardinality	Entropy (in bits)
Arabic numbers (0-9)	10	3.322
Hexadecimal numbers(0-F)	16	4.000
Lower case latin alphabet (a-z)	26	4.700
Case-sensitive latin alphabet (a-z, A-Z)	52	5.700
Case-sensitive alphanumeric (a-z, A-Z, 0-9)	62	5.954
ASCII printable	95	6.570
Diceware word list	7776	12.925

Diceware english word list:

```
...
13314 bang
13315 banish
13316 banjo
13321 bank
13322 banks
13323 bantu
13324 bar
13325 barb
13326 bard
13331 bare
13332 barfly
13333 barge
...
```

User-generated passwords according to NIST Special Publication 800-63:

- the entropy of the first character is taken to be 4 bits,
- the entropy of the next 7 characters are 2 bits per character,
- for the 9th through the 20th character the entropy is taken to be 1.5 bits per character,
- For characters 21 and above the entropy is taken to be 1 bit per character,
- A “bonus” of 6 bits of entropy is assigned for a composition rule that requires both upper case and non-alphabetic characters,
- A “bonus” of up to 6 bits of entropy is added for an extensive dictionary check.

Bruce Schneier (2005):

> *"Simply, people can no longer remember passwords good enough to reliably defend against dictionary attacks, and are much more secure if they choose a password too complicated to remember and then write it down. We're all good at securing small pieces of paper. I recommend that people write their passwords down on a small piece of paper, and keep it with their other valuable small pieces of paper: in their wallet."*

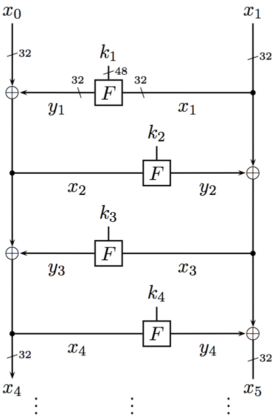
Overview

Dictionary attacks

Exhaustive key search

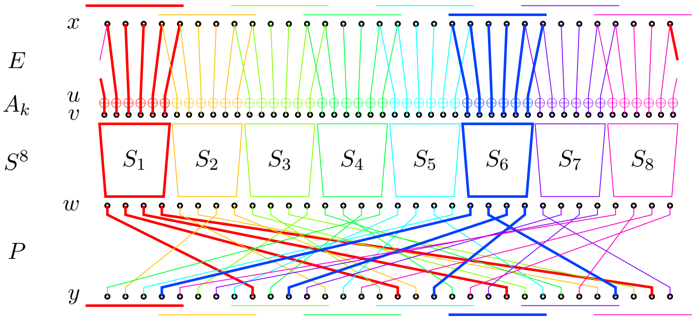
Collision finding

The Data Encryption Standard (DES) was the first modern block cipher, standardized in 1977. It employs a 56-bit key and encrypts 64-bit blocks using a 16 round Feistel network.



We have $y_i = F_{k_i}(x_i)$ and $y_i = x_{i-1} + x_{i+1}$.

The DES F-function looks as follows:



Definition of S_1:

$efgh$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$0efgh0$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
$0efgh1$	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
$1efgh0$	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
$1efgh1$	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

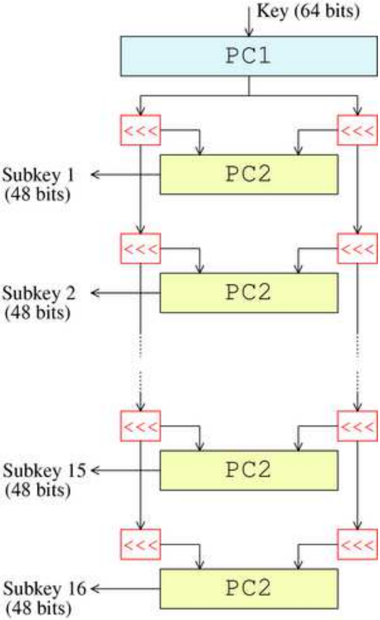
Definition of S_2:

$efgh$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$0efgh0$	F	1	8	E	6	B	3	4	9	7	2	D	C	0	5	A
$0efgh1$	3	D	4	7	F	2	8	E	C	0	1	A	6	9	B	5
$1efgh0$	0	E	7	B	A	4	D	1	5	8	C	6	9	3	2	F
$1efgh1$	D	8	A	1	3	F	4	2	B	6	7	C	0	5	E	9

Definition of S_3:

...

The DES key-schedule looks as follows:



Overview

Dictionary attacks

Exhaustive key search

Collision finding

Birthday paradox

How many randomly chosen people have to be in a room to have a probability of at least 50% that two of them have the same birthday, assuming each birthday occurs with equal probability?

Surprising answer:

23 people are sufficient!

Theorem:

We consider random choices, with replacement, among m labeled items. The expected number of choices until a collision occurs is $O(\sqrt{m})$.

Birthday paradox

How many randomly chosen people have to be in a room to have a probability of at least 50% that two of them have the same birthday, assuming each birthday occurs with equal probability?

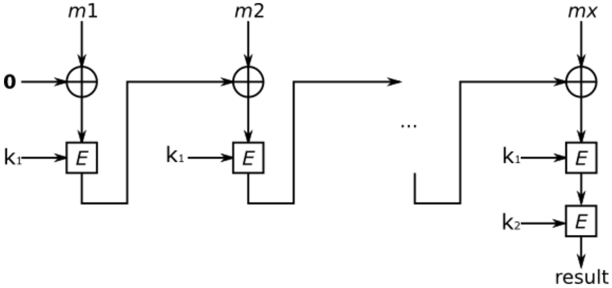
Surprising answer:

23 people are sufficient!

Theorem:

We consider random choices, with replacement, among m labeled items. The expected number of choices until a collision occurs is $O(\sqrt{m})$.

CBC MAC with re-encryption:



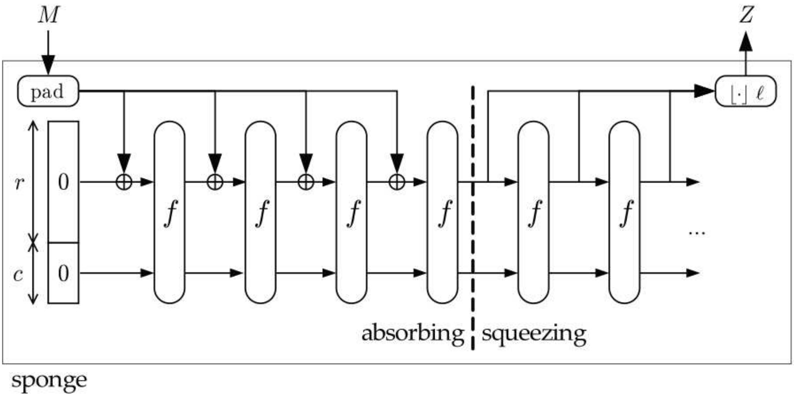
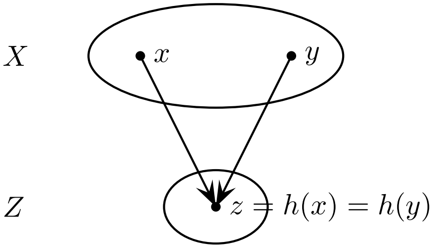


Figure : The SHA-3 sponge construction.


X
x
y
Z
$z = h(x) = h(y)$

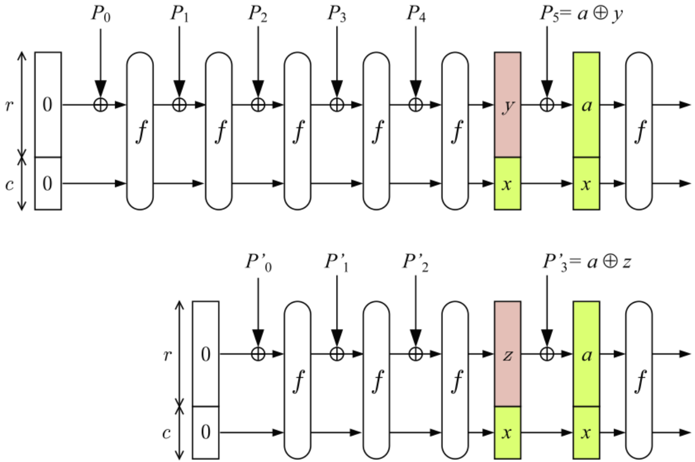


Figure : Collisions in the sponge construction.

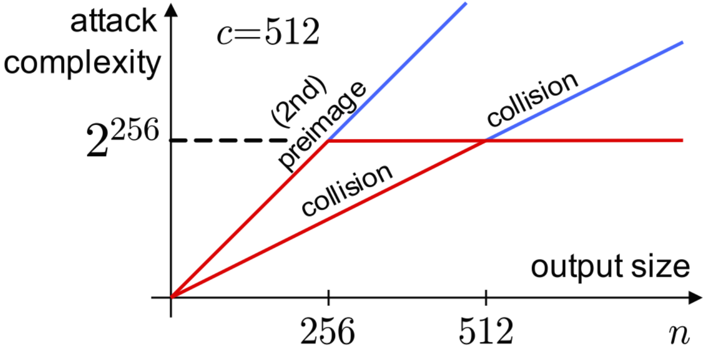


Figure : The sponge claim.

One round of the SHA-3 f function consists of five steps

$$R = \iota \circ \chi \circ \pi \circ \rho \circ \theta,$$

where ι is addition by some round specific constant.

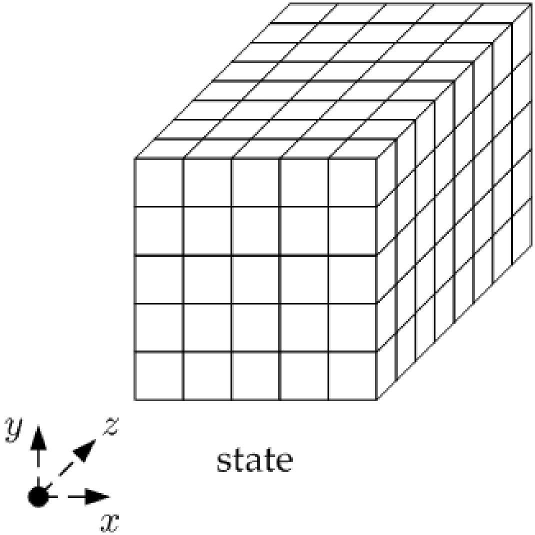


Figure : A state of the SHA-3 f function.

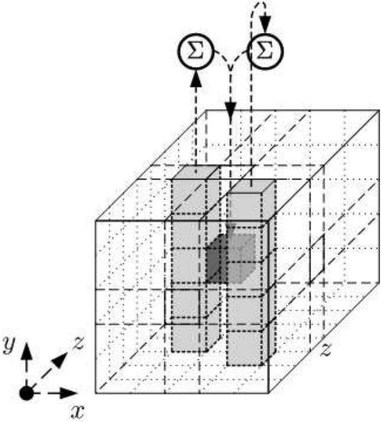


Figure : The step θ in the SHA-3 f function

Compute

$$a[x][y][z] \leftarrow a[x][y][z] + \sum_{y'=0}^{4} a[x-1][y'][z] + \sum_{y'=0}^{4} a[x+1][y'][z-1].$$

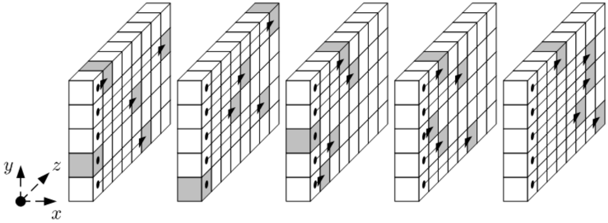


Figure : The step ρ in the SHA-3 f function

Compute

$$a[x][y][z] \leftarrow a[x][y][z-(t+1)(t+2)/2]$$

for some suitably selected $0 \leq t < 24$.

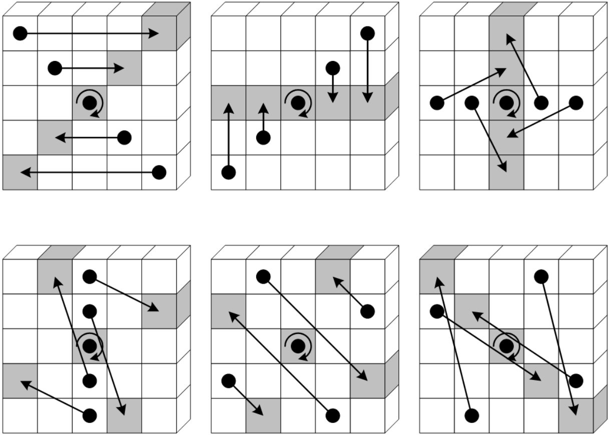


Figure : The step π in the SHA-3 f function

Compute

$$a[x][y] \leftarrow a[x'][y']$$

for some suitably selected x', y'.

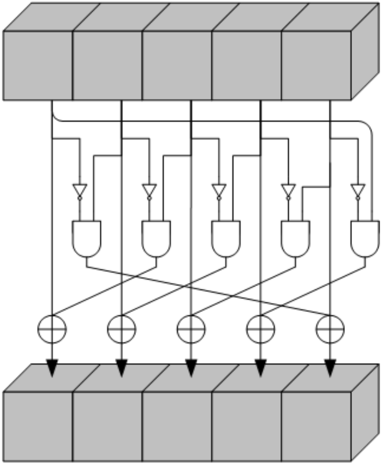


Figure : The step χ in the SHA-3 f function

Compute

$$a[x] \leftarrow a[x] + (a[x+1]+1)a[x+2]$$