30.4.07

2

3.2 (iv), (ii)

3.1 (iii)

AES: why $x^8+x^4+x^3+x+1$?

3.2 ~~(iv)~~ (iii)

$\# \mathbb{Z}^*_{pq} = |\mathbb{Z}^*_{pq}| \leq (p-1)(q-1)$

A: $|\mathbb{Z}^*_{pq}| \geq p \cdot q - p - q + 1$

(ii) $\Rightarrow N_p \cap N_q = \{0\} \Rightarrow |N_p \cup N_q| = p+q-1$

(ii)

$N_p = \{\alpha \in \mathbb{Z}_{pq} \mid \alpha = k \cdot q,\ k \in [1 : p]\}$

N_q

$\mathbb{Z}^*_{pq} \cap (N_p \cup N_q) = \emptyset$ and $\mathbb{Z}_{pq} \supseteq \mathbb{Z}^*_{pq}$

$\Rightarrow |\mathbb{Z}_{pq}| \geq |\mathbb{Z}^*_{pq}| + |(N_p \cup N_q)|$ $\cup (N_p \cup N_q)$

$= |\mathbb{Z}^*_{pq}| + p + q - 1$

A:

$\geq (pq - p - q + 1) + (p + q - 1)$

$= p \cdot q$

30.4.07 5

(iv) $\not\exists_{pq}$: $\exists s,t \in \mathbb{Z}: \quad sq + tp = 1$ (1)

$a \in \mathbb{Z}_{pq}^{*}$ $\exists s',t' \in \mathbb{Z}: \quad s'a + t'pq = 1$ (2)

$p \nmid a$

$1 < q \nmid a$

$q = \dfrac{s'a - 1}{-t'}$

$s''a + t''pq = 1$ (3)

INTEGERS

$$sa + \frac{(tp)q}{q} = 1$$

(4) from 1

$$sa - \frac{tt'pq}{s'a-1} = 1$$

$$\Leftrightarrow sa(s'a-1) - tt'pq = s'a - 1$$

$$\Leftrightarrow s'a - sa(s'a-1) + tt'pq = 1$$

$$\Leftrightarrow \underbrace{(s' + s - ss'a)}_{=s''}a + \underbrace{(tt')}_{t''}pq = 1 .$$

$$\Leftrightarrow (s''a + t''pq) \equiv 1 \pmod{pq}$$

$$\Leftrightarrow \underbrace{s''a \bmod pq}_{=1} + \underbrace{t''pq \bmod pq}_{=0} = 1$$

$$\Leftrightarrow s''a \equiv 1 \pmod{pq}$$

$-t'q = s'a - 1$, $t'q = 1 - s'a$

$t'qsa + t't pq = t'q$

$(1-s'a)sa + t't pq = 1 - s'a$

$(s + s' - s's a)a + t't pq = 1$

$s + s' - s's a =: s''$ $\qquad t''$

So we are done! a is invertible in $\mathbb{Z}_{pq}$.

& $a^{-1} = s''$.

---

1. $\;qsa + tpq = q$
2. $\;psa + t'pq = p$ } ?

$\sigma p + \tau q = 1$ (use p for a in (2) or q for a in (1).)

is

$(\sigma p s' + \tau q s)a + (\tau t + \sigma t')pq = \sigma p + \tau q = 1$

$=: s''$ $\qquad =: t''$.

30.4.07

[5]

$\mathbb{Z}_{26}$ $\quad\cong\quad$ $\mathbb{Z}_2 \times \mathbb{Z}_{13}$

$\mathbb{Z}_2$ \ $\mathbb{Z}_{13}$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0 A	14	2	16	4	18	6	20	8	22	10	24	12
1	13 N	1	15	3	17	5	19	7	21	9	23	11	25

□ = Σ sum

◇ = Π prod.

$\mathbb{Z}_4$ \ $\mathbb{Z}_2$	0	1
0	0/2	
1		1/3

← $\mathbb{Z}_4$?

3.1 (ii) $\quad \mathbb{Z}_2 \times \mathbb{Z}_{13}$

$0 \hat{=} (0,0)$

$13 \hat{=} (1,0)$

A, N

Modulo 2 the plaintexts are different

$\Rightarrow$ a, i are determined mod 2.

But modulo 13 the A and N are indistinguishable

$\Rightarrow$ α not fixed!

3.1 (iii) It suffices to 'track' one row

(because only 1 is inv. mod 2

so only one choice for α mod 2)

and two columns.

Thus 3 pairs are always enough.

(For $35 = 5 \cdot 7$ we would to track two rows and two cols, so 8 are smallest...)