14. JULI 2011

Crypto1 GÜ 11

a.) $p = 3137 \quad a = 9999 \quad b = 1011$

$a^{-1} \pmod{(p-1)}$

$31336 = 3 \cdot 9999 + 1339$

$9999 = 7 \cdot 1339 + 626$

$1339 = 2 \cdot 626 + 87$

$626 = 7 \cdot 87 + 17$

$87 = 17 \cdot 8 + 2$

$17 = 2 \cdot 8 + 1$

$\Rightarrow 1 = 17 - 2 \cdot 8$

$= 17 - (8 - 17 \cdot 8)\, 8$

$= 17 \cdot 41 - 8 \cdot 87$

$= 41 \cdot 626 - 295 \cdot 87$

$= 639 \cdot 626 - 295 \cdot 1339$

$= \underbrace{14767}_{a^{-1}} \cdot \underbrace{9999}_{a} - 4712 \cdot 31336$

$b^{-1} \pmod{(p-1)}$

$= \ldots = \underbrace{-6261}_{b^{-1}} \cdot \underbrace{1011}_{b} + 202 \cdot 31336$

$\Rightarrow -6261 \equiv 25075 \pmod{31336}$

b.) $A \to B : c_1 = m^a \pmod{p} = 6399$ S&M

$B \to A : c_2 = c_1^b \pmod{p} = 29872$

$A \to B : c_3 = c_2^{a^{-1}} \pmod{p} = 24982$

B dec. $m = c_3^{b^{-1}} \pmod{p} = 3567$

	1		3567	S	02868
				S	02968
S	0		667	S	018925
S	0		6271	S	037120
				SM	1 143
S/M	1		23498	SM	1 20384
S/M	1		23177	SM	1 30282
S/M	1		3298	SM	1 6399

Ex37:

Let $n = p \cdot q$, $p \neq q$ be prime and x a non-trivial solution of $x^2 \equiv 1 \pmod{n}$, i.e. $x \not\equiv 1 \pmod{n}$

Then $\gcd(x+1, n) \in \{p, q\}$

$x \not\equiv 1 \pmod{n}$

$\Rightarrow 2 \leq x \leq n-2$

$\Rightarrow x \in \mathbb{Z}^* \setminus \{2, n-2\}$

Proof:

$$x^2 \equiv 1 \pmod{n} \iff (x^2 - 1) \equiv 0 \pmod{n}$$
$$\iff (x+1)(x-1) = 0 \pmod{n}$$
$$\iff (x+1)(x-1) = k \cdot p \cdot q \quad \exists k \in \mathbb{N}$$

$\iff p \cdot q \mid (x+1)(x-1)$

$\iff p$ divides either $(x+1)$ or $(x-1)$

$\iff q$ divides either $(x+1)$ or $(x-1)$

and $x-1 < x+1 < n$ holds:

$\iff p \cdot q \nmid (x+1) \iff p \cdot q > x+1$

$\iff p \cdot q \nmid (x-1) \iff p \cdot q > x-1$

$\iff$ either p or q divide $x+1$

$\Rightarrow \gcd(x+1, n) \in \{p, q\}$

□

Crypto GÜ 11

Ex 38.1

a.) $p = 3571$, $a = 2$, $y = 2905$

- p prime? yes, MRPT or Quadratic Sieve
  $\Rightarrow \sqrt{3571} > 59 \Rightarrow$ try all primes ≤ 59 ✓
- is a a PE?

$$a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod p \quad \forall i$$

$3570 = 2 \cdot 1785 = 2 \cdot 5 \cdot 357 = 2 \cdot 5 \cdot 17 \cdot 21$
(p_1 p_2 p_3 p_4)

$p_i = 2$: $2^{1785} \pmod p = -1$
5: $2^{714} \pmod p = 2910$
17: $2^{210} \pmod p = 1847$
21: $2^{170} \pmod p = 2141$
} $\not\equiv 1$

$\Rightarrow c_1$ is equal for the distinct messages m_1 and m_2
$\Rightarrow$ Alice chose the same session key k twice

b.) $m_1 = 567$ given, known plaintext-attack
$\underline{c_1} = (c_1, c_2)$, $\underline{c_2} = (c_3, c_4)$
same session key k: $c_1 = c_3 = a^k \bmod p$
$y = a^x \bmod p$

$\Rightarrow K = y^k = a^{x \cdot k} \bmod p$ in both cases

$$m_1 = k^{-1} c_2 \pmod p$$

$$\Leftrightarrow k = m^{-1} \cdot c_2 \pmod p \Leftrightarrow k^{-1} = c_2^{-1} m_1 \pmod p$$

$$m_2 = c_4 \cdot k^{-1} \pmod p \Leftrightarrow m_2 = c_4 \cdot c_2^{-1} \cdot m_1 \pmod p$$

$$c_2^{-1} = 347 \mod 3571 \Rightarrow m_2 = 1393 \cdot 567 \cdot 347 \pmod{3571}$$

$$= 274071357 \pmod{3571}$$

$$= 678 \pmod{3571}$$