Crypto 2 Ü5

Ex 14.)

1.) Factorize $n = 1333$, quadratic sieve:

$\Rightarrow \sqrt{1333} > 36$

$p = 35$? try $p = p - 2$

$p = 33, \underline{\underline{31}}$

$$n = \underbrace{31}_{=p} \cdot \underbrace{43}_{=q} = \underline{1333}$$

2.) Compute $d_1 = \left(\frac{p+1}{4}\right)^{t+1} \bmod (p-1) = 8^{10} \bmod 30 \equiv 4$

$$d_2 = \left(\frac{q+1}{4}\right)^{t+1} \bmod (q-1) = 11^{10} \bmod 42 \equiv 25$$

$$u = x_{t+1}^{d_1} \bmod p \equiv 1306^4 \bmod 31 \equiv 8$$

$$v = x_{t+1}^{d_2} \bmod q \equiv 1306^{25} \bmod 43 \equiv 4$$

Compute the inverses: $ap + bq = 1$

$43 = 31 \cdot 1 + 12 \quad \Rightarrow \quad 1 = 5 - 2 \cdot 2$

$31 = 12 \cdot 2 + 7 \qquad = 5 - 2(7-5)$

$12 = 7 \cdot 1 + 5 \qquad = 3 \cdot 5 - 2 \cdot 7$

$7 = 5 \cdot 1 + 2 \qquad = \ldots$

$5 = 2 \cdot 2 + \underline{\underline{1}} \qquad = 3 \cdot 12 - 5 \cdot 7$

$= 13 \cdot 12 - 5 \cdot 31$

$= \underbrace{13}_{b} \cdot \underbrace{43}_{q} - \underbrace{18}_{a} \cdot \underbrace{31}_{p}$

$$x_0 = (v \cdot a \cdot p + u \cdot b \cdot q) \bmod n$$

$= (4 \cdot (-18) \cdot 31 + 8 \cdot 13 \cdot 43) \equiv -2232 + 4472$

$\equiv 907 \bmod 1333$

Compute $x_1, \dots, x_9$ with $x_{i+1} \equiv x_i^2 \pmod{n}$

x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
907	188	686	47	876	901	4	16	256	219

$(10\underbrace{11110}_{b_0}0)_2$ last 5 digits of the binary representation

i	1	2	3	4	5	6	7	8	9
c_i	10101	01110	00011	01000	10111	00101	11110	01101	11000
b_i	11100	01110	01111	01100	00101	00100	10000	00000	11011
m_i	01001	0000	01100	00100	10010	00001	01110	01101	00011
	J	A	M	E	S	B	O	N	D

$m_i = c_i \oplus b_i \quad \forall i = 1, \dots, 9$ // $h = \lfloor \log \lfloor \log n \rfloor \rfloor = 3 < \underline{5}$

<u>Ex 15.)</u>

In a BG cryptosystem: $n = p \cdot q$, $p \neq q$, $\underbrace{p, q \equiv 3 \bmod 4}$ // Blum-numbers

- Given an arbitrary ciphertext: $(c_1, \dots, c_t, x_{t+1})$
→ the decoding-hardware produces: $(m_1, \dots, m_t)$ but not x_0

→ we know that $b_i = m_i \oplus c_i$, $1 \le i \le t$

→ By assumption, we have that $\mathcal{L}(\underbrace{b_i}_{\text{last 5 bits of } x_i}) = \overset{\text{a QR mod } n}{x_i}$, $1 \le i \le t$

We obtain a sequence of consecutive squares and also their QRs.

$x_t^2 = x_{t+1}$, $x_{t-1}^2 = x_t$, ...

As in p75 of the lecture notes, the attacker selects ~~..~~ a random $r \in \mathbb{Z}_n^*$ and computes/deciphers $x'_{t+1} \equiv r^2 \pmod n$

With a pos. probability: $x_t' \not\equiv \pm r \bmod n$

// if $x_t \equiv \pm r \bmod n$ repeat

Using prop. 6.8. (security of the Rabin cryptosystem):

$\Rightarrow$ compute $\gcd(x_t' - r, n) \in \{p, q\}$, n is factorized.

Ex 16.)

a.) In an RSA cryptosystem $n = p \cdot q$, $q \neq p$
$e \in \mathbb{Z}_{\varphi(n)}$ $\gcd(e, \varphi(n)) = 1$

$$\varphi(n) = (p-1)(q-1)$$

public key (n, e)

1.) generator: random seed $\Rightarrow x_0 \in \{2, \dots, n-1\}$, $e \in \mathbb{Z}_{\varphi(n)}$
2.) compute (iterate) $x_{i+1} = x_i^e \pmod n$, $1 \le i \le t$ //RSA-encryption
3.) b_i last $k = \lfloor \log \lfloor \log(n) \rfloor \rfloor$ of x_i
4.) pseudorandom sequence: $b_1, b_2, \dots, b_t$
DLP (x_{t+1}, e)