Public Key Encryption

- One-way function : $n = p \cdot q$ | n given, $p, q = ?$

→ RSA cryptosystem :

p, q prime, $n = p \cdot q$, e , $d = e^{-1} \bmod (p-1)(q-1)$

public key : n, e

private key : d

encryption : $c = m^e \bmod n$

decryption : $m = c^d \bmod n$

- One way function :

p prime , a PE mod p : $y = a^x \bmod p$ | y given, $x = ?$

→ Diffie-Hellman key exchange :

$A: \; u = a^x \bmod p \leftrightarrow B: \; v = a^y \bmod p$

joint key : $a^{xy} \bmod p = a^{yx} \bmod p$

- One way function :

p, q prime , $n = p \cdot q$: $y = x^2 \bmod n$ | given y , $x = ?$

→ Rabin cryptosystem :

<u>Prop. 9.2.</u> $p > 2$ prime.

c is QR mod $p \iff c^{(p-1)/2} \equiv 1 \pmod{p}$ ┘

<u>Prop. 9.3.</u> p prime, $p \equiv 3 \pmod{4}$, i.e., $p = 4k-1$,
c QR mod p. Then
$x^2 \equiv c \pmod{p}$ has the only solutions $x_{1,2} = \pm c^k \bmod p$. ┘

<u>Remark:</u> For $p \equiv 1 \pmod{4}$ there is no known efficient deterministic alg. for solving $x^2 \equiv c \pmod{p}$. However, there is an efficient probabilistic algorithm.

<u>Prop. 9.4.</u> Let $p \neq q$ prime, $n = p \cdot q$.
Compute by the extended Euclidean alg $s, t \in \mathbb{Z}$ with

$$\underbrace{sp}_{=b} + \underbrace{tq}_{=a} = \gcd(p,q) = 1.$$

Let $a = tq$, $b = sp$, further $x, y \in \mathbb{Z}$ with

$$\begin{aligned} x^2 &\equiv c \pmod{p} \\ y^2 &\equiv c \pmod{q} \end{aligned} \qquad (*)$$

Then $f = ax + by$ is a solution of $f^2 \equiv c \pmod{n}$. ┘

RWTH AACHEN UNIVERSITY

<u>Proof.</u> By definition

$a \equiv 1 \pmod p$, $b \equiv 0 \pmod p$

$a \equiv 0 \pmod q$, $b \equiv 1 \pmod q$

Moreover

$$(ax+by)^2 \equiv a^2x^2 + 2abxy + b^2y^2$$
$$\equiv \begin{cases} x^2 \equiv c & \pmod p \\ y^2 \equiv c & \pmod q \end{cases}$$

By Prop. 8.1 $(ax+by)^2 \equiv c \pmod n$. $\boxed{\equiv}$

Remark: There are 4 solutions to $x^2 \equiv c \pmod n$, if $n = p \cdot q$, $p \neq q$ prime.

<u>Rabin Cryptosystem</u>

(i) $p \neq q$ prime, $n = p \cdot q$, $p, q \equiv 3 \pmod 4$

(ii) Public key: n, private key: (p, q)

(iii) Encryption: $c = m^2 \bmod n$ (message m)

(iv) Decryption: Determine $x : x^2 \equiv c \pmod p$

$y : y^2 \equiv c \pmod q$

Use Prop. 9.4. <u>OR</u>

4 solutions, choose the one where the last 64 bits are identical, e.g., to the previous ~~last~~ 64 bits, because they have been replicated before encrypting.

OR Determine $f \equiv x \pmod p$
$f \equiv y \pmod q$

by the Chinese Remainder Theorem.

(4 solutions as well)

$$\left.\begin{array}{ll} f^2 \equiv x^2 \equiv c & \pmod p \\ f^2 \equiv y^2 \equiv c & \pmod q \end{array}\right\} \Rightarrow f^2 \equiv c \pmod n.$$

Bear in mind: $m \gg \sqrt{n}$, otherwise a solution is obtained by computing square root over $\mathbb{R}$.

Remark 9.5. 4 solutions! Identify the right one. ⌟

Remark 9.6. (Security of the Rabin system)

a) From Prop 8.1: Breaking "Rabin" is equivalent to factoring.

b) The Rabin system is vulnerable against chosen-ciphertext attack.

- O/E chooses m at random, computes $c = m^2 \bmod n$.
- c is deciphered with plaintext m'.
- With prob. $\frac{1}{2}$: $m' \neq \pm m$. In this ~~ca~~ case computes $\gcd(m-m', n) \in \{p, q\}$ (*)

  Otherwise, repeat the above.

Hence, never publish a deciphered message which is not the original one.

Why is (*):

$x^2 \equiv y^2 \pmod n$, $x \not\equiv \pm y \pmod n$

$\Rightarrow \gcd(x-y, n) \in \{p, q\}$

Since $n \mid x^2 - y^2 \Rightarrow n \mid (x-y)(x+y)$

but $n \nmid (x-y)$ and $n \nmid (x+y)$ $\quad \lrcorner$

c) Broadcast endagers the Rabin system.

The same message m is sent to k receivers $1, \dots, k$, encrypted by public keys $n_1, \dots, n_k$.

$$c_1 = m^2 \bmod n_1$$
$$\vdots$$
$$c_k = m^2 \bmod n_k$$

(Very likely all prime factors in $n_1, \dots, n_k$ are different.)

O/E eavesdrop and solve

$$x \equiv c_1 \pmod{n_1}$$
$$\vdots$$
$$x \equiv c_k \pmod{n_k}$$

The Chinese Rem. Th. yields a solution

$$x \equiv m^2 \pmod{n_1 \cdots n_k}$$

Since $m < n_i$ $\forall i = 1, \ldots, k$, it follows $m^2 < n_1 \cdots n_k$.
Hence $x = m^2$ can be solved for m over $\mathbb{R}$.

The same attack can be applied to RSA for small e.

11 Signature Schemes

Requirements (same as on conventional signatures)

- verifiable
- forgery-proof
- firmly connected to the document

11.1. El Gamal signature scheme

h: hash function ✓

Parameters: p: prime, a PE mod p

Select random x, $y = a^x \bmod p$

Public key: (p, a, y) Private key: x

Signature generation:

Select random k s.t. $k^{-1} \bmod (p-1)$ exists.

$r = a^k \bmod p$

$s = k^{-1}(h(m) - xr) \bmod (p-1)$

Signature for m: (r, s)

Signature verification:

Verify $1 \leq r \leq p-1$

$$v_1 = y^r r^s \bmod p$$

$$v_2 = a^{h(m)} \bmod p$$

$v_1 = v_2 \longrightarrow$ accept signature.

Verification works:

$$ks \equiv h(m) - xr \pmod{p-1}$$

$$\Leftrightarrow \quad h(m) \equiv xr + ks \pmod{p-1}$$

$$\Leftrightarrow \quad xr + ks = \ell(p-1) + h(m) \text{ for some } \ell \in \mathbb{Z}$$

Hence

$$\begin{aligned} y^r r^s &\equiv a^{xr} a^{ks} \equiv a^{xr+ks} \\ &\equiv a^{\ell(p-1)} a^{h(m)} \\ &\equiv \underbrace{(a^{p-1})}_{\equiv 1 \pmod p \text{ (Fermat)}}{}^{\ell} \cdot a^{h(m)} = a^{h(m)} \pmod p. \end{aligned}$$

∎