Rabin cryptosystem

Prop. 9.3. If $p \equiv 3 \pmod 4$ prime, i.e., $p = 4k-1$, c QR mod p then
$x^2 \equiv c \pmod p$ has solutions $x_{1,2} = \pm c^k \bmod p$ ⌋

Th. 6.10. Chinese Remainder Theorem

$$x \equiv a_i \pmod{m_i}, \quad i = 1, \dots, r$$

has a unique solution mod $M = \prod_{i=1}^{r} m_i$, namely

$$x = \sum_{i=1}^{r} a_i M_i y_i \pmod M,$$

$M_i = M/m_i$, $y_i M_i^{-1} \bmod m_i$. ⌋

Rabin Cryptosystem

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

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

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

Decryption:

Solve $x^2 \equiv c \bmod p$ by Prop. 9.3

$y^2 \equiv c \bmod q$

Determine $f \equiv x \pmod p$

$f \equiv y \pmod q$

by the CRT Th. 6.10.

Then $f^2 \equiv x^2 \equiv c \pmod{p}$

$f^2 \equiv y^2 \equiv c \pmod{q}$

Prop. 8.1 $\Rightarrow$ $f^2 \equiv c \pmod{p \cdot q}$

There are 4 solutions f, one is the message m. ⊣

Obsve that $m \gg \sqrt{n}$, otherwise

$m^2 \bmod n = m^2 < n$

Deciphering by comp. squ. root over $\mathbb{R}$.

Remark 9.5. The "right" message must be identified. To achieve this repeat the last 64 bits of the message.

Remark 9.6. (Security)

a) From Prop. 8.2: Breaking the Rabin system is equivalent to factoring.

b) Rabin system is vulnerable against chosen ciphertext attacks:

- O/E choose m at random, compute $c = m^2 \bmod n$.
- c is deciphered with plaintext m'.
- With probability $\frac{1}{2}$: $m' \neq \pm m$.
  Then compute $\gcd(m-m', n) \in \{p, q\}$ (*)
  Otherwise repeat the above.

(*) $x^2 \equiv y^2 \pmod n$, $x \not\equiv \pm y \pmod n$
$\Rightarrow \gcd(x-y, n) \in \{p, q\}$
Since $n \mid x^2 - y^2 \Rightarrow n \mid (x+y)(x-y)$
$n \nmid (x-y)$, $n \nmid (x+y)$.

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

c) Broadcast endangeres the Rabin system.
The same message m is sent to K receivers $1, \dots, K$ with public keys $n_1, \dots, n_K$.

$$c_1 = m^2 \bmod n_1$$
$$\vdots$$
$$c_K = m^2 \bmod n_K$$

Very likely that $n_1, \dots, n_K$ are pairwise relatively prime.

O/E eavesdrops the channels and solves

$$x \equiv c_1 \pmod{n_1}$$
$$\vdots$$
$$x \equiv c_K \pmod{n_K}$$

The CRT 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 $x = m^2$, m may be computed as squ. root in $\mathbb{Z}$. ⊣

11. Signature Schemes

Electronic signature on a message.

Requirements (same as on conventional signatures)

- verifiable (proof of ownership)
- forgery proof
- firmly connected to the document

Problem for certain applications: repeated use of copies.

Attacks on signature schemes:

- key only attack
- known message attack
- chosen-message attack

Different kinds of breaking

- Total break
- Selective forgery
- Existential forgery

8.1.3. The RSA signature scheme

Normally, the document m is first compressed to a short string $h(m)$ by a so called hash function h. h is a one-way function.

RSA signature, approved by NIST in Dec. 1998.

Alice uses public key $(d_A^{-1} = e_A, n_A)$, private key d_A.

Signature generation on message m:

$$s = (h(m))^{d_A} \bmod n_A$$

s: signature on m.

Verification of s by B

$$g = s^{e_A} \bmod n_A \quad \text{(using A's public key)}$$

If $h(m) = g$, B accepts A's signature.

Security

a) B cannot change m to $\tilde{m}$, otherwise $h(\tilde{m}) \neq s^{e_A} \bmod n_A$.
B cannot generate a valid signature on $\tilde{m}$, since d_A is private.

b) A "random" hash h can be generated as

$$h = s^{e_A} \bmod n_A$$

with valid signature s, since

$$h^{d_A} \equiv s \pmod{n_A}.$$

h will be meaningless with high probability.