RSA speed

RSA is ~ 1000 times slower than DES in hardware.
and ~ 100 times slower than DES in software.

8.1.2. Implementation of RSA

- large prime numbers p, q → MRPT
- Choice of $d \in \mathbb{Z}^*_{\varphi(n)}$ → start with some odd d_0
  $d_0 \leftarrow d_0 + 2$
  until $gcd(d_0, \varphi(n)) = 1$
  or choose prime number d, if $d > \max\{p, q\}$
- Inverse $d^{-1} \pmod{\varphi(n)}$ → EEA
- Exponentiation → SQM
- Table concerning RSA hardware, see Schneier p. 469

8.1.3 The RSA signature scheme

Method of signing digital messages m → digital signature

Requirements (same as on conventional signatures)
- verifiable (proof of ownership)
- forging-proof
- firmly connected to the document

Usually, a document is first compressed to a short string, which is signed → Hash functions h (AMC)

RSA signature, approved by NIST since Dec. 1998

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

Signature generation on message m. A computes

$$s = (h(m))^{d_A} \mod n_A \qquad \text{(using the private key)}$$

s signature on m

Verification of s by B. B computes

$$g = s^{e_A} \mod n_A \qquad \text{(Using A's public key)}$$

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

(By Prop 8.2: If s is a valid signature on $h(m)$ then $g = h(m)$)

Security

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

b) A "random" hash g can be generated as
$$g = s^{e_A} \mod n_A$$
with valid signature s, since $g^{d_A} \equiv s \pmod{n_A}$
g will be meaningless with high probability.

8.2 The El Gamal Cryptosystem

Secrecy is based on the discrete logarithm problem

El Gamal System

(i) Public : p : large prime number , α : PE $(\mathrm{mod}\ p)$

(ii) Private key : some random secret $x \in \{2, \dots, p-2\}$

Public key : $y = \alpha^x \bmod p$

(iii) Message $m \in \{1, \dots, p-1\}$

Encryption : Choose some random secret $k \in \{2, \dots, p-2\}$

Compute $K = y^k \bmod p$

$C_1 = \alpha^k \bmod p$, $C_2 = K \cdot m \bmod p$

Decryption : $C_1^x \bmod p \overset{(*)}{=} K$

$m = K^{-1} C_2 \bmod p$

$(*)$ hold since $C_1^x = (\alpha^k)^x \bmod p = (\alpha^x)^k \bmod p = y^k \bmod p = K$

(C_1, C_2) is the ciphertext

Remarks :

a) A second key k is chosen (by the sender). The same plaintext can have different ciphertext.

b) Relation to Diffie-Hellman scheme : joint key is K $[= (\alpha^k)^x \bmod p]$. C_1 is the "public key" of the sender. Encryption of m by multiplication by K.

c) Breaking El Gamal is equivalent to solving the DH problem

8.3 Generalized ElGamal Encryption

ElGamal encryption works in any cyclic group G. Security is based on the intractability of the discrete logarithm problem in G.

List of groups that are appropriate

i) $\mathbb{Z}_p^*$, p is prime

ii) $\mathbb{F}_{2^m}^*$, the multiplicative group of the finite field $\mathbb{F}_{2^m}$, $m \in \mathbb{N}$

iii) Group of points on an elliptic curve (see AMC)

iv) $\mathbb{F}_{p^m}^*$, the multiplicative group of the finite field $\mathbb{F}_{p^m}$, p prime, $m \in \mathbb{N}$

Generalized ElGamal system

(i) Select ~~a~~ a cyclic group G of order n, with a PE a (G is written multiplicatively)

(ii) Select a random secret integer x $1 \le x \le n-1$

Compute $y = a^x$ in G

Public key: a, y, description G

Private key: x

(iii) Encryption: Represent the message as $m \in G$

Select a random integer k $1 \le k \le n-1$

Compute: $K = y^k$

$$c_1 = a^k, \quad c_2 = K \cdot m$$

(c_1, c_2) is the ciphertext

(iv) Decryption

Compute $c_1^x \; (= a^{kx} = y^k = K)$

$$m = c_1^{-x} c_2 = K^{-1} c_2$$

Example : $G = \mathbb{F}_{2^4}^*$

Elements are polynomials of degree ≤ 3 over $\mathbb{F}_2$. Multiplication modulo the irreducible polynomial $f(u) = u^4 + u + 1$

The elements $a_3 u^3 + a_2 u^2 + a_1 \cdot u + a_0 \in \mathbb{F}_{2^4}$ is represented by the binary string $(a_3\, a_2\, a_1\, a_0)$

G has order 15, $a = (0010)$ is a generator

verification that a is a generator, as $\{u^k \mid k = 1, \dots, 15\} = \mathbb{F}_{2^4}^*$

$u,\ u^2,\ u^3,\ u+1,\ u^2+u,\ \underset{(6)}{u^3+u^2},\ \underset{(7)}{u^3+u+1},\ \underset{(8)}{u^2+1},\ u^3+u,$
$u^2+u+1,\ \underset{(11)}{u^3+u^2+u},\ u^3+u^2+u+1,\ \underset{(13)}{u^3+u^2+1},$
$u^3+1,\ 1$

- A chooses $x = 7$

  A's public key $a = (0010)$, $\gamma = a^7 = (1011)$

- Encryption

  $m = (1100) = a^6$

  B selects $k = 11$, $K = \gamma^{11} = (a^7)^{11} = a^{15 \cdot 5 + 2} = a^2 = (0100)$

  $C_1 = a^{11} = (1110)$

  $C_2 = K \cdot m = a^2 \cdot a^6 = a^8 = (0101)$

  $C(C_1, C_2) = (a^{11}, a^8)$

- Decryption

  A computes $C_1^x = (0100) = a^2 = K$

  $K^{-1} = a^{13} = (1101)$

  $m = K^{-1} C_2 = a^{13} \cdot a^8 = a^6 = (1100) = m$ ✓

9.2 The Rabin cryptosystem (Rabin, 1979)

In principle like RSA with public key $e = 2$
However $\nexists d : d \cdot e \equiv 1 \pmod{\varphi(n)}$, since $\gcd(e, \varphi(n)) = 2 \neq 1$
Deciphering means to compute square roots modulo n.
But computing square roots is no easier than factoring $\rightarrow$ Prop 8.3
Computing square roots mod p, p is prime is easy.

<u>Def. 9.1</u> c is called <u>quadratic residue</u> mod n (QR mod n)
if $\exists x : x^2 \equiv c \pmod{n}$

<u>Prop 9.2</u> (Euler's criterion)
Let $p > 2$, prime: c is QR mod p $\Leftrightarrow$ $c^{(p-1)/2} \equiv 1 \pmod{p}$
<u>Proof</u>: Ex.

In general Prop 9.2 provides no indication how to compute square roots

<u>Prop 9.3</u> Let 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>Proof</u>: $k = \frac{p+1}{4}$

$$(x_{1,2})^2 \equiv (c^k)^2 \equiv c^{(p+1)/2} \equiv c \cdot \underbrace{c^{(p-1)/2}}_{\equiv 1 \pmod{p}\ (9.2)} \equiv c \pmod{p}$$

Assume $x^2 \equiv c \pmod{p}$ and $y^2 \equiv c \pmod{p}$

$\Rightarrow x^2 - y^2 \equiv 0 \pmod{p} \Rightarrow p \mid (x-y)(x+y)$

$\Rightarrow p \mid (x+y)$ or $p \mid (x-y) \Rightarrow x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$

Hence, $x_{1,2}$ are the <u>only</u> solutions.