S_5/ RSA (classical case)

B = Bob

A = Alice

I. • B chooses $p \neq q$ primes; compute $N = pq$ and $\varphi(N) = (p-1)\cdot(q-1)$

• B chooses $1 < e < \varphi(N)$ with $\gcd(e, \varphi(N)) = 1$

• B computes (using fast exponentiation alg.) $0 < d < \varphi(N)$

such that $ed \equiv 1 \pmod{\varphi(N)}$

$\hookrightarrow d = e^{-1} \pmod{\varphi(N)}$

=> public key (N, e)

private key (N, d)

II Encryption

$\mathcal{P} = \{ m \in \mathbb{N} : 1 < m < N \}$

• A computes $c = m^e \pmod N$

III Decryption

• B computes $m = c^d \pmod N$

Ex. 1 Consider $N = 85$

A -> public key $e = 3$

-> sends $m = 80$

Find: a) cyphertext

b) secret key

c) decrypt the message

Sol.:

a) $c = m^e \pmod N$ | $\Rightarrow c = 80^3 \pmod{85}$

$m = 80$ | $= (-5)^3 \pmod{85}$

$e = 3$ | $= 45 \pmod{85}$

$N = 5$

b) $d \cdot e = 1 \pmod{\varphi(N)}$

$d = e^{-1} \pmod{\varphi(N)}$

$d = 3^{-1} \pmod{\varphi(N)}$

$N = 85 = 5 \cdot 17 \Rightarrow \varphi(N) = 4 \cdot 16 = 64$

$d = 3^{-1} \pmod{64}$

Euclid alg. (extended version)

$64 = 3 \cdot 21 + 1$

$1 = 64 - 3 \cdot 21 \pmod{64}$

$1 = 3 \cdot (-21) \pmod{64}$

$\Rightarrow 3^{-1} = 43 \pmod{64}$

$\Rightarrow d = 43$

c) $\left.\begin{array}{l} c = 45 \\ d = 43 \end{array}\right\} \Rightarrow m = c^d \pmod N$

$m = 45^{43} \pmod N$

-> fast exponentiation algorithm

$43 = 32 + 8 + 2 + 1$

$45^1 = 45 \pmod{85}$
$45^2 = 70 \pmod{85} = (-15) \pmod{85}$
$45^4 = 55 \pmod{85}$
$45^8 = 50 \pmod{85}$
$45^{16} = 35 \pmod{85}$
$45^{32} = 35 \pmod{85}$

$m = 45^1 \cdot 45^2 \cdot 45^8 \cdot 45^{32} \pmod{85}$

$= 45 \cdot 70 \cdot 50 \cdot 35 \pmod{85}$

$= 80 \pmod{85}$

Ex. 2 The same message m is enclypted using RSA and send to both A and B.

Public key A: $(1591, 17)$
Public key B: $(1591, 5)$

Oscar intercepts $c_1 = 849$ (from A)
$c_2 = 22$ (from B)

How could Oscar find m?

Sol.:

$N = 1591$

$A : (N, e_A) = (N, 17)$

$B : (N, e_B) = (N, 5)$

$c = m^e \pmod{N}$

$$\begin{cases} c_1 = m^{e_A} \\ c_2 = m^{e_B} \end{cases} \pmod{N} \iff \begin{cases} 849 = m^{17} \\ 22 = m^5 \end{cases}$$

$\exists\, \alpha_1, \alpha_2 \in \mathbb{Z}$ such that $17\alpha_1 + 5\alpha_2 = 1$

Euclid alg.

$17 = 5 \cdot 3 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2$

$1 = 5 - (17 - 5 \cdot 3) \cdot 2$

$1 = 5 \cdot 7 - 17 \cdot 2$

$\Rightarrow \alpha_1 = -2$

$\alpha_2 = 7$

we know that $5 \cdot 7 + (-2) \cdot 17 = 1$

$$m = m^1 = m^{5 \cdot 7 + (-2) \cdot 17} = m^{5 \cdot 7} \cdot m^{(-2) \cdot 17}$$

$$= (m^5)^7 \cdot (m^{17})^{-2}$$

$$= 22^7 \cdot 849^{-2}$$

$22^7 \rightarrow$ fast exponentiation $\Rightarrow 22^7 = 816$

$849^{-1} \rightarrow$ extended Euclid alg. $\Rightarrow 849^{-1} = 684$

$m = 816 \cdot 684^2 = 500 \pmod N$

<u>Def.</u>: We say that a number is square free if there is no square different than 1 to divide it.

- $\mathrm{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$
- Let n to be square free and $n = p_1 p_2 - p_K$

  Define

  $\lambda(n) = \mathrm{lcm}(p_1 - 1, p_2 - 1, \dots, p_K - 1)$

The Generalisation Fermat Little Theorem

Let N square free and $e = a\lambda(n) + 1$. Then

$\forall x \in \mathbb{Z} \quad x^e = x \pmod N$

RSA$_m$ (modified version)

In the modified case, instead of $\varphi(N)$ we use $\lambda(N)$.

d) $m = c^d \pmod N$

$m = 44^{29} \pmod N$

$\rightarrow$ fast exp. alg. $\Rightarrow m = 11 \pmod{119}$

El Gamal

- A sends m to B ; $m \in \{0, 1, \dots, p-1\}$

I) · A generates randomly a prime number p

- — " — $x \bmod p$
- She chooses $a \in \mathbb{Z}$ $\quad 1 < a \leq p-2$
- Compute $x^a \pmod p$
- Obtain
  - $\rightarrow$ public key (p, x, x^a)
  - $\rightarrow$ private key a

II Encryption

- B choose $b < p-1$, $b \in \mathbb{N}$
- Compute $x^b \pmod p$ and $m x^{ab} \pmod p$
- Cyphertext: $c = (x^b, m x^{ab})$

III Decryption

- $(x^b)^{-a} = (x^b)^{p-1-a} \pmod p$
- $(x^b)^{-a} m x^{ab} = m x^{ab-ab} = m$

El Gamal multiplicative

- Ours mod 11
- Generator $g = 2$
- Secret key $k = 9$ (A)
- B key $y = 7$
- B send $m = 8$

$x = g$
$a = k$
$b = y$

Do the computation.

Sol.:

The public key: $h = g^k \pmod p$

$h = 2^9 \pmod{11}$

$\rightarrow$ fast exp. alg. $\Rightarrow h = 6 \pmod{11}$

h and g are public

$c = (c_1, c_2) = (g^y, m h^y) = (2^7, 8 \cdot 6^7) = (7, 9) \bmod 11$