RSA - Video 1

$\overbrace{p=2, \quad q=7}^{\text{Bob}}$ Choose

$N = 14$; $\varphi(N) = 1 \cdot 6$

2

$m = c \leftarrow 3$

Public Key: Bob: (e, N) $(5, 14)$ $Enc(m) = m^e$

where $(e, \varphi(N)) = 1$

$(5, 6) = 1.$

$3^5 \equiv 9 \cdot 9 \cdot 3 \; (14)$.

$\equiv (-3) \cdot 3 \; (14)$

$$\equiv 5\ (14)$$

$$5 = Enc(m) \leftarrow \text{Ciphertext}$$

Alice $\xrightarrow{\text{Public Channel}}$ Bob

$\qquad\qquad 5$

$m = 3$

$$(e,\ \varphi(N)) = 1.$$

$$5 \cdot 5 \equiv 1\ (6)$$

$$5^5 \equiv 25 \cdot 25 \cdot 5\ (14)$$

$$\equiv (-3)(-3)(5)$$

$$\equiv (-5)(5)$$

$$\equiv 3 \pmod{14}$$

$$\downarrow$$

$$m \leftarrow \text{Bob}.$$

Video2

$$m^{ed} \equiv m \pmod{N} \leftarrow \underline{\text{Prove}}$$

$$(e, \varphi(N)) = 1$$

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

$$\Rightarrow \varphi(N)k + 1 = ed.$$

$$m^{ed} = m^{\varphi(N)k} \cdot m$$

$$(p-1)(q-1)k \quad m$$

$$pq$$

<u>Case 1</u> $(m, N) = 1$.

$$m^{p-1} \equiv 1 \ (p) \Rightarrow m^{\overbrace{(p-1)(q-1)}^{\varphi(N)}} \equiv 1 \ (p)$$

$$m^{q-1} \equiv 1 \ (q)$$

$$m^{\varphi(N)} \equiv 1 \ (p)$$

$$m^{\varphi(N)} \equiv 1 \ (q)$$

$$m^{\varphi(N)} \equiv 1 \ (N)$$

$$m^{\varphi(N)k} \equiv 1 \ (N)$$

$$m^{ed} = m^{\varphi(N)k} \cdot m \equiv 1 \ (N)$$

<u>Case 2</u> $(m, N) \neq 1$.

$$N = pq$$

$$p \mid m$$

$$m^{ed} \equiv 0 \ (p)$$

$$\equiv m \ (p)$$

If $(q, m) \neq 1$

$\varphi(N)k+1$ $\underline{m^{ed}} = m$

$\equiv \underline{m} \ (q)$.

$m^{ed} \equiv m \ (N)$.

Video3

Prove: $m^{p-1} \equiv 1 \ (p)$; $\forall m$, $(m, p) = 1$.

p - prime.

$G = \mathbb{Z}_p^{\times} = \{ a \in [1, p-1] ; (a, p) = 1 \}$

a, b

ab

$m \in G$, $\# G = p - 1$.

$a \in G$, $\# G = n$

Then $g^n = 1$; $\forall g \in G$.

Video 4

El Gamal Encryption

p - prime.

$\mathbb{Z}_p^\times = \langle g \rangle$

$x \in \mathbb{Z}_p^\times = \{1, \ldots, p-1\}$

$x < p-1$. , x secret

Bob.

$$\boxed{y_{(p)} = g^x}$$

$(p, g, y) \to$ Public Key.

Bob do this

Alice wants to send message $m \in \mathbb{Z}_p = \{0, \dots, p-1\}$.

$c_1 = g^k$

$k \in \{1, \dots, p-2\}$

$c_2 = m \cdot y^k$

$Enc(m) = (c_1, c_2) \leftarrow$ Ciphertext

$\downarrow$ Public Channel.

Bob.

$$s = c_1^{x} \pmod{p} \qquad g^{kx}$$

$$c_2 \, s^{-1} \overset{?}{=} m g^{k - kx} \quad (g$$

$$= m \pmod{p}$$

Video 5

Diffie-Hellmann Key Exchange.

Alice $\quad$ $g \in [N]$, 5 $\quad$ Bob.

PUBLIC CHANNEL

$4 = a$ $\qquad\qquad$ $b = 3$

ag $\longrightarrow$ bag = K

abg $\longleftarrow$ bg //

K

Video 6

Oblivious Transfer.

Random

Alice

N, e

Bob

m_0, m_1

b, k

x_0

x_1

R d random

Public

Channel

$$P_0 = (V - x_0)^d$$
$$P_1 = (V - x_1)^d$$

$$V = x_b + k^e \pmod N$$

$$m_0' = m_0 + P_0 \pmod N$$

$$m_1' = m_1 + P_1 \pmod N$$

$$m^* = m_b' - k$$

$$= m_b + (V - x_b)^d - k$$

Alice chose e, d in a way that

$$de \equiv 1 \pmod N \;;\; \forall a < N \;;\; (a, n) = 1$$

$$= m_b + k^{ed} - k \quad a$$

$$= m_b + k - k$$

$$= m_b$$

~~(Mod N)~~

Algorithm

1. Alice choose N, e such that

$$(e, \varphi(N)) = 1.$$

She computed d such that

$$ed \equiv 1 \ (\varphi(N))$$

2. Bob choose the bit $b \in \{0, 1\}$. and he choose k such that $(k, N) = 1$

3. Alice sends Randomly choosen X_0, X_1

4. Bob chooses X_b based on the choice of b he made.

5. Bob computes

$$V = (X_b + k^e) \bmod N$$

V sends to Alice

6. Alice does $P_0 = (V - X_0)^d \ (\bmod N)$

$$P_1 = (V - x_1)^d \pmod N$$

7. Alice sends

$$m_0' = m_0 + P_0 \pmod N$$
$$m_1' = m_1 + P_1 \pmod N$$

8. Bob computes

$$m^* = m_b' - k$$

$$= (m_b + P_b - k)$$

Using 6. $= m_b + (V - x_b)^d - k$

Using 5. $= m_b + k^{ed} - k.$

Since $ed \equi 1 \ (\varphi(N))$ & $(k, N) = 1$

$$RHS = m_b + k - k$$
$$= m_b \pmod{N}$$

Hence, Bob knows the message m_b & he has no idea about m_{1-b} at all.