

## RSA - Video 1

$p=2, q=7$  Bob Choose ^

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

$m = 3$  ← 2  
Pub (e, N) ← 3  
Bob (e, N) Enc (m) =  $m^{e \text{ key}}$   
where  $(5, 14)$  ←  
 $(e, \varphi(N)) = 1$

$$(5, 6) = 1.$$

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

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

$$\equiv 5(14)$$

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

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

$$m=3$$

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

$$5 \cdot 5 \equiv 1 \pmod{6}$$

$$5^5 \equiv 25 \cdot 25 \cdot 5 \pmod{14}$$

$$\bar{3} \cdot (-3) \cdot 5$$

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

$$\equiv 3(14)$$

↓

$m \leftarrow \text{Bob.}$

Video 2  
ed

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

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

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

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

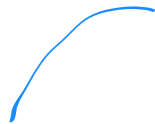
$$\varphi(N)k m^{\text{ed}} = m \cdot m$$



1

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

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



Case 2  $(m, N) \neq 1$ .

$$N = pq$$

$$p \mid m$$

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

$$\equiv m(p)$$

IF

$$(q, m) \neq 1$$

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

$$\equiv \underline{m}(1).$$

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

Video 3

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

$p$  - prime.

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

$a, b$

$ab$

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

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

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

## Video 4

## El Gamal Encryption

$p$ -prime.

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

$$x \in \mathbb{Z}_p^* = \{1, \dots, p-1\}$$

$x < p-1$ ,  $x$  secret  
└─ Bob.

$$y = g^x$$

$(p, g, y) \rightarrow \text{Public Key.}$

Bob do this

Alice wants to send

message  $m \in$

$\mathbb{Z}_p = \{0, \dots, p-1\}$

$c_1 = g^m$   
 $k \in \{1, \dots, p-2\}$

$$c_2 = m \cdot y^k$$

$\text{Enc}^{(m)} = (c_1, c_2) \leftarrow \text{Ciphertext}$

$\downarrow$  Public Channel.

Bob.

Q

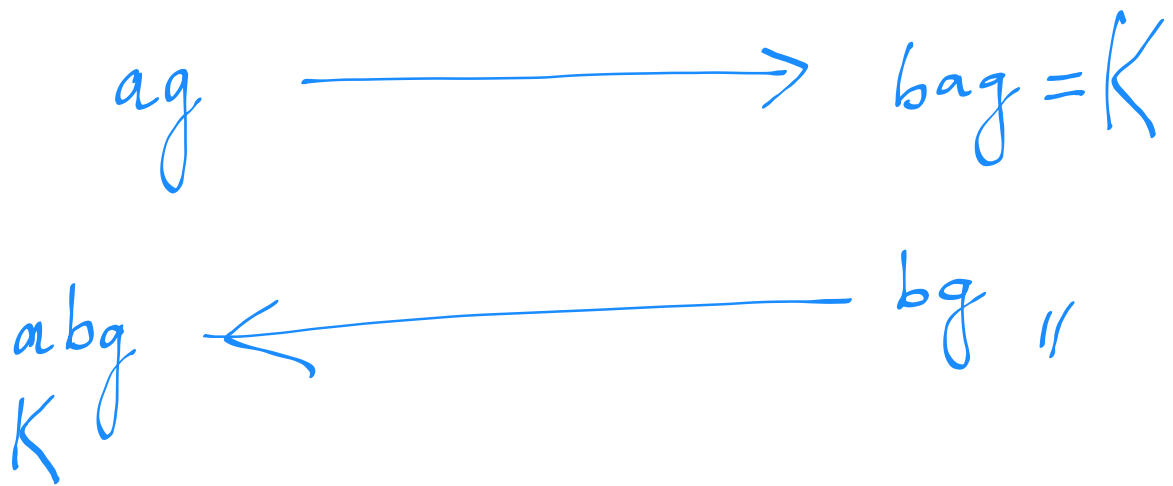


$$\begin{aligned}
 s &= c_1^x \pmod{p} & g^{kx} \\
 c_2 s^{k-xA} &= m g^x \pmod{p} \\
 &= m \pmod{p}
 \end{aligned}$$

## Video 5

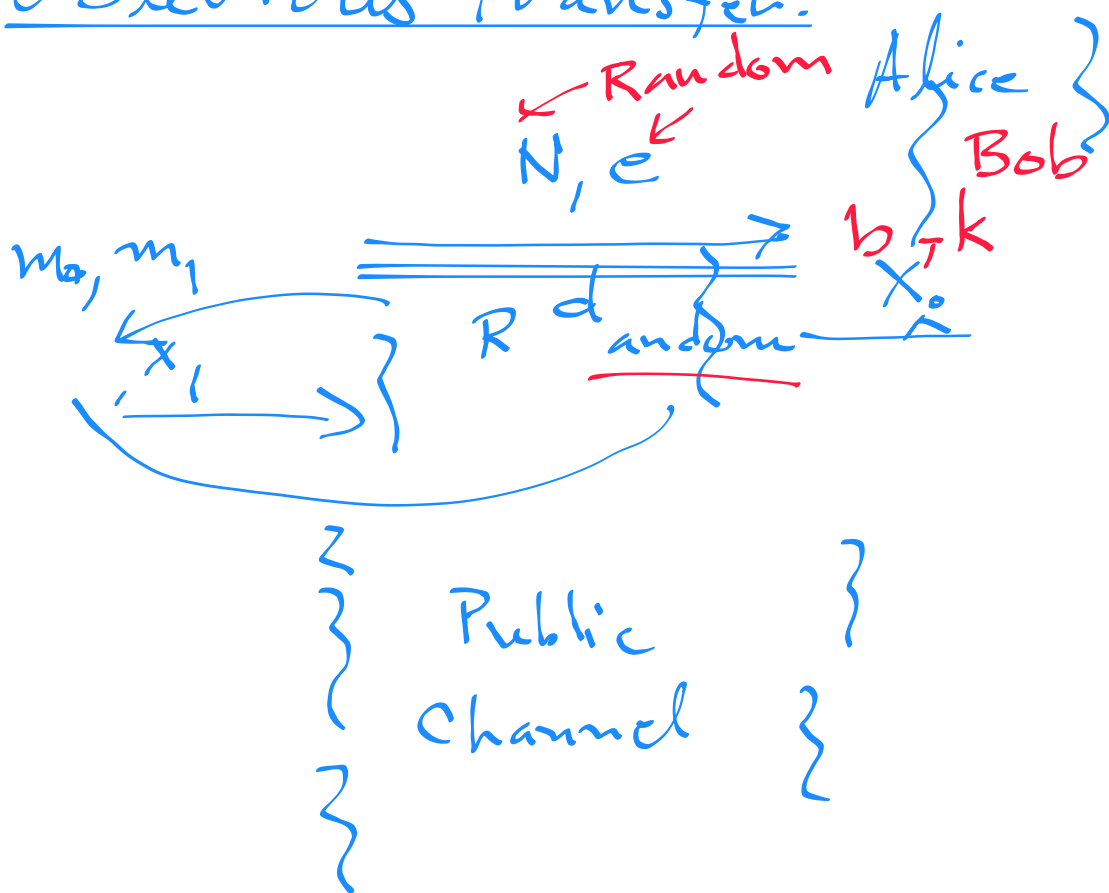
Diffie-Hellman Key Exchange.

Alice	<sup>5</sup> " $g \in [N]$ "	Bob.
~~~~~		
PUBLIC CHANNEL		
$4 = a$		$b = 3$



## Video 6

### Oblivious Transfer.



$$\begin{aligned}
 P_0 &= (V - X_0)^d \\
 P_1 &= (V - X_1)^d \\
 V &= X_b + k^e \pmod{N} \\
 m'_0 &= m_0 + P_0 \pmod{N} \\
 m'_1 &= m_1 + P_1 \pmod{N} \\
 m^* &= m'_b - k \\
 &= m_b + (V - X_b)
 \end{aligned}$$

Alice chose  $e, d$  in a way that

$$\begin{aligned}
 &ed \equiv 1 \pmod{N} \\
 &; \forall a < N; (ea)^d = 1
 \end{aligned}$$

(Mod N) Algorithm

$$\begin{aligned}
 &= m_b + k^{ed} - k \quad a \\
 &= m_b + k - k \\
 &= m_b
 \end{aligned}$$

1. Alice choose  $N, e$  such that

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

She computed  $d$  such that

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

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

3. Alice sends Randomly chosen  
 $X_0, X_1$

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  $P_0 = (V - X_0) \pmod{N}$

$$P_i = (V - X_i)^d \pmod{N}$$

7. Alice sends

$$m'_0 = m_0 + P_0 \pmod{N}$$

$$m'_1 = m_1 + P_1 \pmod{N}$$

8. Bob computes

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

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

$$\text{Using 6.} \quad = m_b + (V - X_b)^d - k$$

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

$$\text{Since } ed \equiv 1 \pmod{\phi(N)} \text{ \& } (k, N) = 1$$

$$\begin{aligned} \text{RHS} &= m_b + k - k \\ &= m_b \pmod{N} \end{aligned}$$

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