

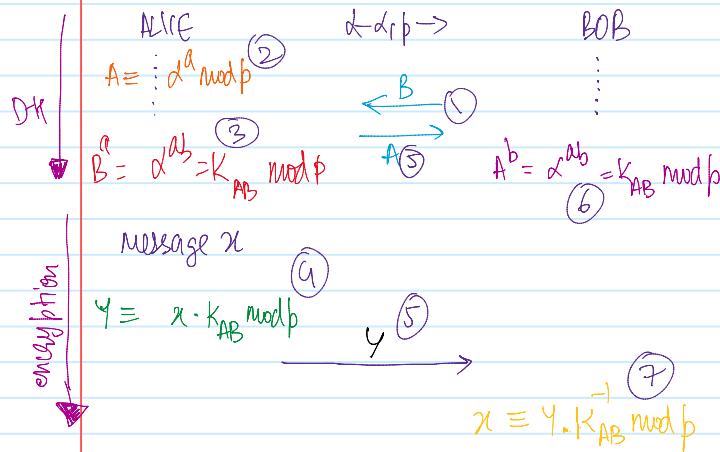
# Elgamal Encryption Scheme

Saturday, 7 December 2019 3:13 PM

## ENCRYPTION WITH DLP:

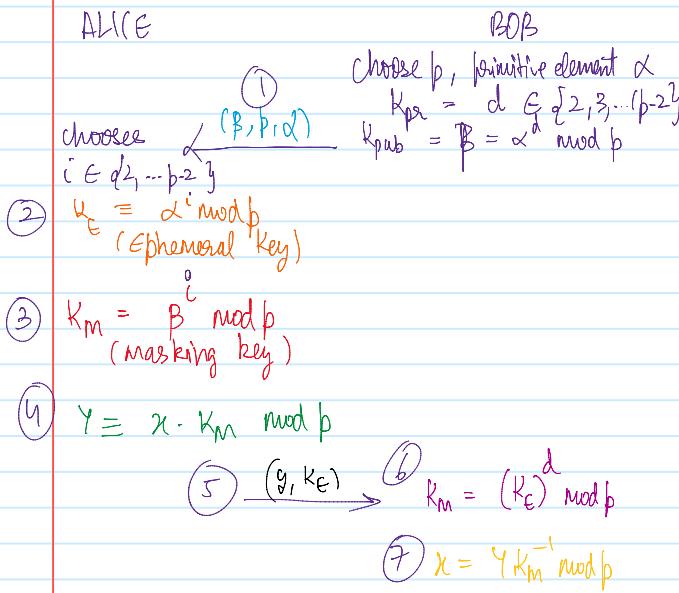
SERVICE	Algorithmic Family		
	Integer Factor	DH	DLP
Key exchange	RSA	D-H	ECOM
Digital Signature	RSA	Egamil	ECDSA
Encryption	RSA	Egamil	ECX

Goal: Develop Encryption scheme from D-H Key Exchange



## ELGAMAL ENCRYPTION

- invented around 1985
- very similar to D-H but reordering of steps
- also spelled as ELgamal.



Proof of correctness:

$$\text{Bob computes: } \dots \dots -1 \quad (x - d)^{-1} \quad \dots \dots$$

## Remarks:

(1) Advantage of Elgamal over direct D-H encryption:

Bob's public key is fixed and  $\alpha, p$  are chosen by him.

(2)  $K_E$  must be different for every plaintext.  $K_E \neq B$  (randomiser)

$$(3) \begin{array}{ccc} x & \rightarrow & e(\cdot) \\ y = x_i & \rightarrow & \boxed{e(\cdot)} \\ & & \downarrow \\ & & x_i \end{array}$$

No, because  $i$  changes every time  $\Rightarrow K_E$  changes  $\Rightarrow Y_2 \neq Y_1$

∴ Elgamal is a "PROBABILISTIC" ENCRYPTION scheme unlike schoolbook RSA

## COMPUTATIONAL ASPECTS:

Alice and Bob have to compute

$$\begin{aligned} B &= \alpha^d && \text{SQUARE AND} \\ K_E &= \alpha^i && \text{MULTIPLY} \\ K_m &= \beta^i && \text{ALGORITHM} \end{aligned}$$

$$\begin{aligned} \text{Q: } (1) \quad K_m &\equiv K_E^d \text{ mod } p \\ (2) \quad K_m^{-1} &\equiv \text{extended euclidean} \end{aligned}$$

we can merge (1) and (2)

by Fermat's little theorem

$$K_E \in \mathbb{Z}_p^* : K_E^{p-1} \equiv 1 \text{ mod } p$$

$$\begin{aligned} K_m^{-1} &\equiv (K_E^d)^{-1} \cdot 1 \\ &= K_E^{-d} \cdot K_E^{p-1} \\ &= K_E^{p-1-d} \text{ mod } p \end{aligned}$$

Step (7) becomes

$$x = y K_m^{-1} \equiv y K_E^{p-1-d} \text{ mod } p$$

## ATTACKS

parameters that Oscar doesn't know are  $i$  and  $d$

(1) compute DLP

$$d = \log_{\alpha} B$$

& then he can do same as Bob  $\rightarrow K_m = K_E^d ; x \equiv y K_m^{-1}$

(2)

$$i = \log_{\alpha} K_E$$

$$\rightarrow K_m = B^i ; x \equiv y K_m^{-1}$$

∴ DLP needs to be a computational hard problem

proof of correctness:

Bob computes:

$$y \cdot K_m^{-1} = y \cdot (K_E^d)^{-1} \pmod{p}$$

$$\equiv x \cdot K_m \cdot K_E^{-d} \pmod{p}$$

$$\equiv x \cdot \beta^i \cdot (\alpha^i)^{-d} \pmod{p}$$

$$\equiv x \cdot (\alpha^d)^c \cdot (\alpha^i)^{-d} \pmod{p}$$

$$\equiv x \cdot \alpha^{id} \cdot \alpha^{-id} \pmod{p}$$

$$\equiv x \cdot \alpha^{id-id} \pmod{p}$$

$$\equiv x \pmod{p}$$

DLP needs to be a computational hard problem  
 $\therefore p$  must be large  $p \geq 2^{1024}$

### ② Attack Re-use of secret exponent $i$

$$K_E = \alpha^i, \quad K_m = \beta^i$$

$$y_1 = x_1 \cdot K_m \xrightarrow{(y_1, K_E)}$$

$$y_2 = x_2 \cdot K_m \xrightarrow{(y_2, K_E)}$$

assume: Oscar knows  $x_1$ .

(is a known PLAINTEXT)

$$K_m = y_1 \cdot x_1^{-1} = y_2 \cdot x_2^{-1}$$

$$y_2 \equiv y_2 \cdot y_1^{-1} \cdot x_1 \pmod{p}$$