Extra week #10

14 de dezembro de 2025 18:43

Q3: ElGamal

P1) From the $Enc(X, m)$ algorithm we get (Y, c), and we know that

$(Y \leftarrow g^y)$ $(c \leftarrow m \cdot s)$

From the $Dec(x, (Y, c))$ algorithm we get the message

$(m \leftarrow c \cdot s^{-1})$ $(s \leftarrow Y^x)$

$m \leftarrow c \cdot s^{-1} \iff m \leftarrow (m \cdot s) \cdot s^{-1} \iff m \leftarrow m \cdot s^{1-1}$

$\iff m \leftarrow m \cdot s^0 \iff m \leftarrow m$ (*)

But why are the s value from $Enc(X, m)$ and from $Dec(x, (Y, c))$ the same? Let's see why

$Enc(X, m)$:

$s = X^y$; $X \leftarrow g^x$

so $s \leftarrow (g^x)^y \iff \boxed{s \leftarrow g^{xy}}$

$Dec(x, (Y, c))$:

$s = Y^x$; $Y \leftarrow g^y$

$s \leftarrow (g^y)^x \iff s \leftarrow g^{yx} \iff \boxed{s \leftarrow g^{xy}}$

exactly the same

Since the shared secret calculated is the same, what is shown in (*) answers the question P1

P2) In this context we know that "hardness" means that the resources required to reverse the math are greater than any attacker possesses.

This hardness comes from inversing $X \leftarrow g^x$ or inversing $Y \leftarrow g^y$

We know that $m \leftarrow c \cdot s^{-1}$ and $s \leftarrow Y^x$ so we need the value of s to get the message but get it would mean to recover in some way the value of x or y (because we already know (X, Y and g).

Calculating x from $X \leftarrow g^x$ or Y from $Y \leftarrow g^y$ is completely unfeasible.

Worth mentioning that recovering y from $Y \leftarrow g^y$ is the Discrete Logarithm Problem which is computationally unfeasible for large numbers.

Not having a way of getting m without the private key is what answers confidentiality.

P3) The attacker gets c of message m

$c \leftarrow m \cdot s$ $s \leftarrow X^y$ $s \leftarrow Y^x$

Then, the attacker can compute

$c' \leftarrow c \cdot K \pmod q$, $K \in \mathbb{Z}$

If we send (Y, c') to the Dec function we get

$m' \leftarrow c' \cdot s^{-1} \iff m' \leftarrow c \cdot K \cdot s^{-1} \iff$

$\iff m' \leftarrow m \cdot s \cdot K \cdot s^{-1} \iff m' \leftarrow m \cdot K$

We've successfully changed the value of the resulted decrypted message in a predictable way.

Proving that ElGamal is malleable.