Cyber-Security — Tutorial N°3

Exercise 1:

[Challal 2016] We want to design a secure data exchange protocol. The protocol must guarantee the following security services:

— Confidentiality

— Integrity

— Non-repudiation

We assume that confidentiality is ensured by symmetric encryption and initially, the two communicating parties do not share any secret key. Write a specification of this protocol using the following notations:

- A ==> B : M (A sends M to B)
- $\{M\}_K$: M encrypted/decrypted with K
- SK_X : private key of X
- PK_X : public key of X
- K_{AB} : secret key shared between A et B
- H (m): Hash code of message m
- **.** : Concatenation between two parts of a message

Exercise 2 :

[Challal 2016] We consider the following cryptographic protocol:

M1 : B ==> A : B . PKb

M2 : A ==> B : {m} PKb

This protocol is vulnerable to Man in the Middle attack. An intruder "I" can attack this protocol as follows:

- ☐ I intercepts M1

  I blocks M1

  I replaces M1 by : M1 : I ==> B : A.PKi

  I intercepts M2

  I blocks M2

I replaces M2 by : M2 : I ==> A : {m}PKa

- I intercepts M1

  I blocks M1

  I replaces M1 by : M1 : I ==> A : B.SKb

  I intercepts M2

  I blocks M2

  I replaces M2 by : M2 : I ==> B : {m}PKb

- I intercepts M1

  I blocks M1

  I replaces M1 by : M1 : I ==> A : B.PKi

  I intercepts M2

  I blocks M2

  I replaces M2 by : M2 : I ==> B : {m}PKb

Exercise 3:

Let X and Y be two entities wishing to exchange encrypted messages using a symmetric cryptosystem. X and Y must both agree on the same symmetric key K_{XY} that is *n* bits long.

- X chooses a random number C and a partial key K_X then sends $K_X \oplus C$ to Y.

  X ➔Y : $K_X \oplus C$

- Y chooses K_Y and responds by $K_X \oplus C \oplus K_Y$.

  Y ➔ X : $K_X \oplus C \oplus K_Y$

- Finally, X responds by $C \oplus K_Y$.

  X ➔Y : $C \oplus K_Y$

C, K_X and K_Y are all *n* bits long.

The secret key shared between X and Y: $K_{XY}=K_X \oplus K_Y$

1- Show how X and Y can both find the key K_{XY}.

2- Is this protocol secure (i.e. an attacker who can spy on all the messages exchanged can find the Key K_{XY}) ?.

3- Is this protocol vulnerable to Man in the middle attack? Explain.