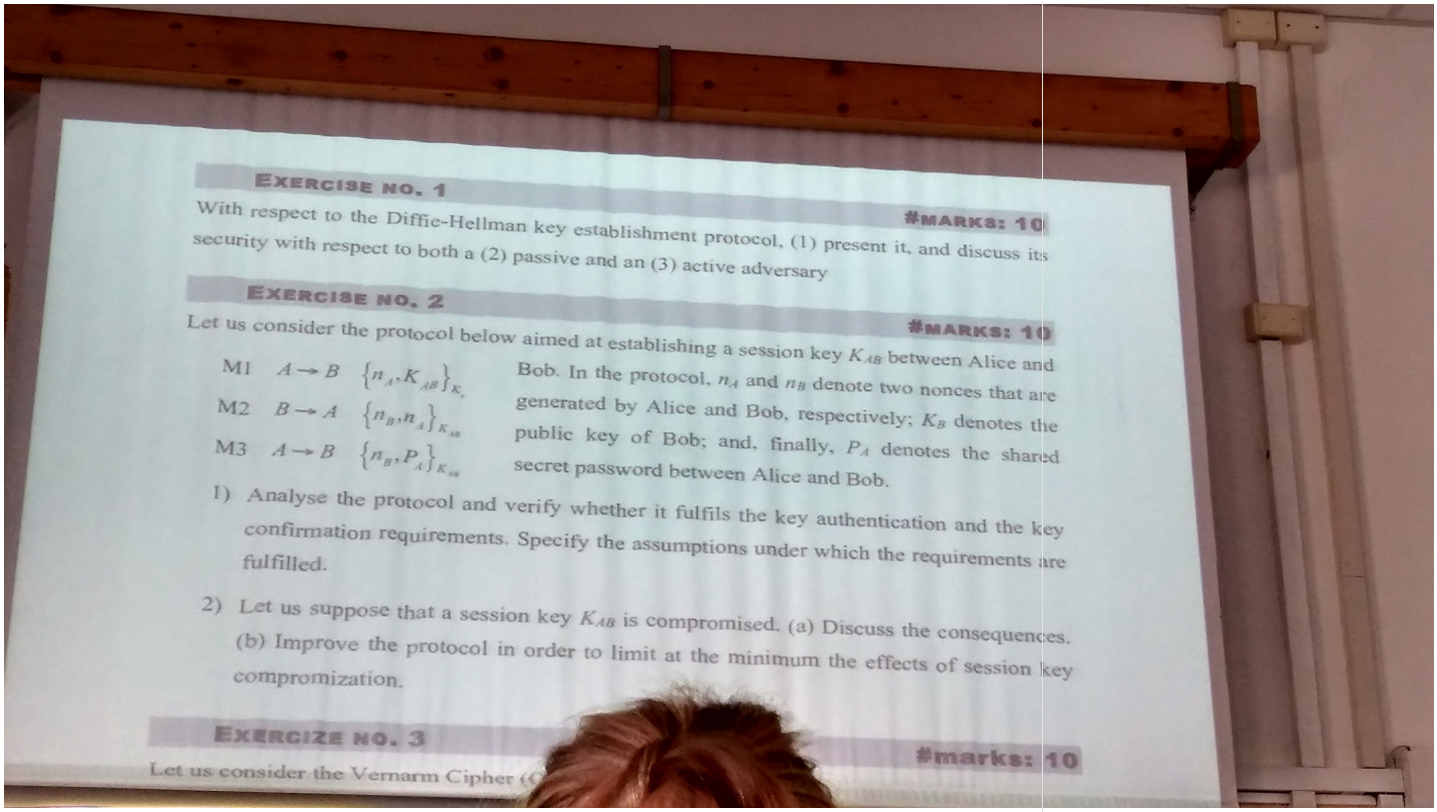
July 6th, 2012

giovedì 25 maggio 2017 11:18



EXERCISE NO. 1

#MARKS: 10

With respect to the Diffie-Hellman key establishment protocol, (1) present it, and discuss its security with respect to both a (2) passive and an (3) active adversary

EXERCISE NO. 2

#MARKS: 10

Let us consider the protocol below aimed at establishing a session key K_{AB} between Alice and Bob. In the protocol, n_A and n_B denote two nonces that are generated by Alice and Bob, respectively; K_B denotes the public key of Bob; and, finally, P_A denotes the shared secret password between Alice and Bob.

M1 $A \rightarrow B$ $\{n_A, K_{AB}\}_{K_B}$

M2 $B \rightarrow A$ $\{n_B, n_A\}_{K_{AB}}$

M3 $A \rightarrow B$ $\{n_B, P_A\}_{K_{AB}}$

1) Analyse the protocol and verify whether it fulfils the key authentication and the key confirmation requirements. Specify the assumptions under which the requirements are fulfilled.

2) Let us suppose that a session key K_{AB} is compromised. (a) Discuss the consequences. (b) Improve the protocol in order to limit at the minimum the effects of session key compromization.

EXERCIZE NO. 3

#marks: 10

Let us consider the Vernarm Cipher (

Exercise 2

! • M1 is encrypted by means of K_B

My guess

1. Key confirmation is provided by M3 because A encrypts it by means of K_{ab}
   Key authentication is provided by M3 because A inserts P_A in the message.
2. K_{AB} compromised:
   a. ...
   b. ...

BAN logic

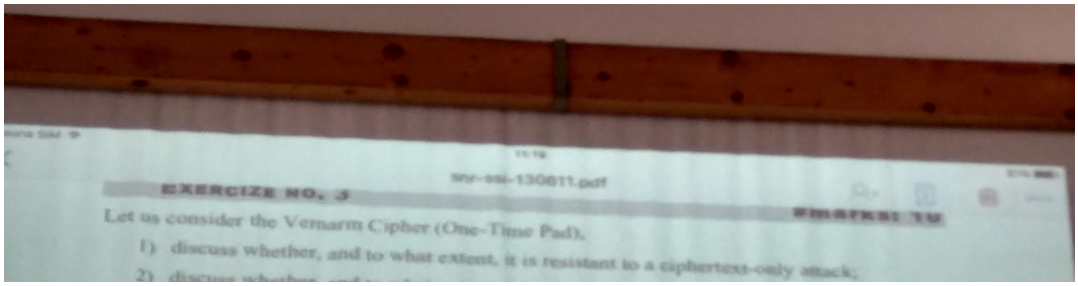
July 17th, 2012

1. Dopo M1, Bob non può sapere da chi sta arrivando, non si può applicare il primo postulato (Bob doesn't believe, it just sees).
   Non ha nessun belief su K_{AB}, e nemmeno sulla sua freschezza, perché n_A non è gestito da Bob.
2. Bob encripta M2 K_{AB} assumendo che solo Alice lo abbia.
   Stesso errore in old SSL.
   Un avversario potrebbe ri-eseguire lo stesso protocollo con K_{AB} tutte le volte che vuole.
   a. Perdendo K_{AB}, si perdono le sessioni passate, a meno che non si utilizzino sessioni ephemeral.
      Perdendo K_{AB}, si perdono le sessioni future.

   b. Ad esempio, P_A si potrebbe inserire subito in M1.
      Per dichiarare la freschezza di M1, Bob potrebbe inviare un nonce in M0.

M0	B → A	n_B
M1	A → B	$\{n_A,\ n_B,\ P_A,\ K_{AB}\}_{K_B}$
M2	B → A	$\{n_A,\ n_B\}_{K_{aB}}$
M3	A → B	$\{n_B,\ n_A\}_{K_{aB}}$

Con K_{AB} compromessa, all'avversario manca comunque la password P_A.
Se K_{AB} viene compromessa, viene compromessa però anche la password P_A.

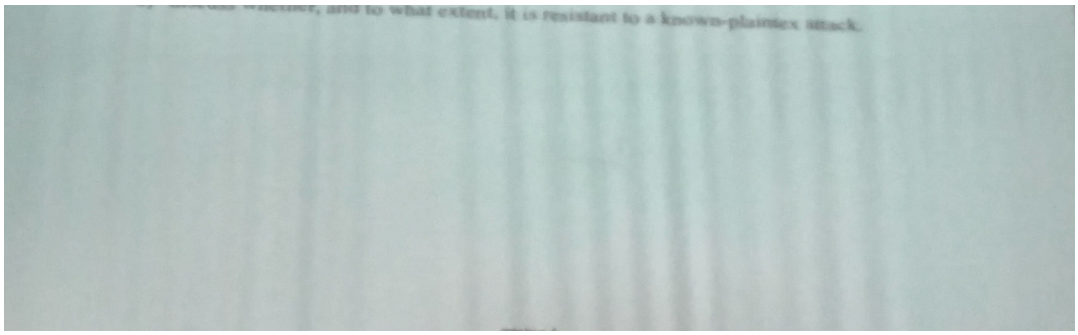


EXERCIZE NO. 3

#marks: 10

Let us consider the Vernarm Cipher (One-Time Pad).

1) discuss whether, and to what extent, it is resistant to a ciphertext-only attack;


whether, and to what extent, it is resistant to a known-plaintext attack.