CORSO DI SICUREZZA INFORMATICA 1 (A.A. 2006/2007)

Prof. A. Armando

(14 Giugno 2007)

Si risponda alle domande utilizzando lo spazio apposito.
Non è consentito l'utilizzo di libri, appunti, nè dispositivi elettronici di alcun tipo.

Nome e Cognome: _____

Matricola: _____

---

1. ***Crittografia simmetrica***

   Si assuma di avere una conoscenza parziale del seguente plaintext e del corrispondente ciphertext:

   Plaintext: `*UA**IAI**ERI**E`
   Ciphertext: `I*ECFA**OH*CKSP*`

   dove $\star$ indica i caratteri non noti.

   Si sa che il ciphertext è ottenuto dal plaintext applicando l'algoritmo di Vigenère con lunghezza del blocco pari a 4 e utilizzando l'alfabeto inglese (ovvero `ABCDEFGHIJKLMNOPQRSTUVWXYZ`*). Si determini la chiave.*

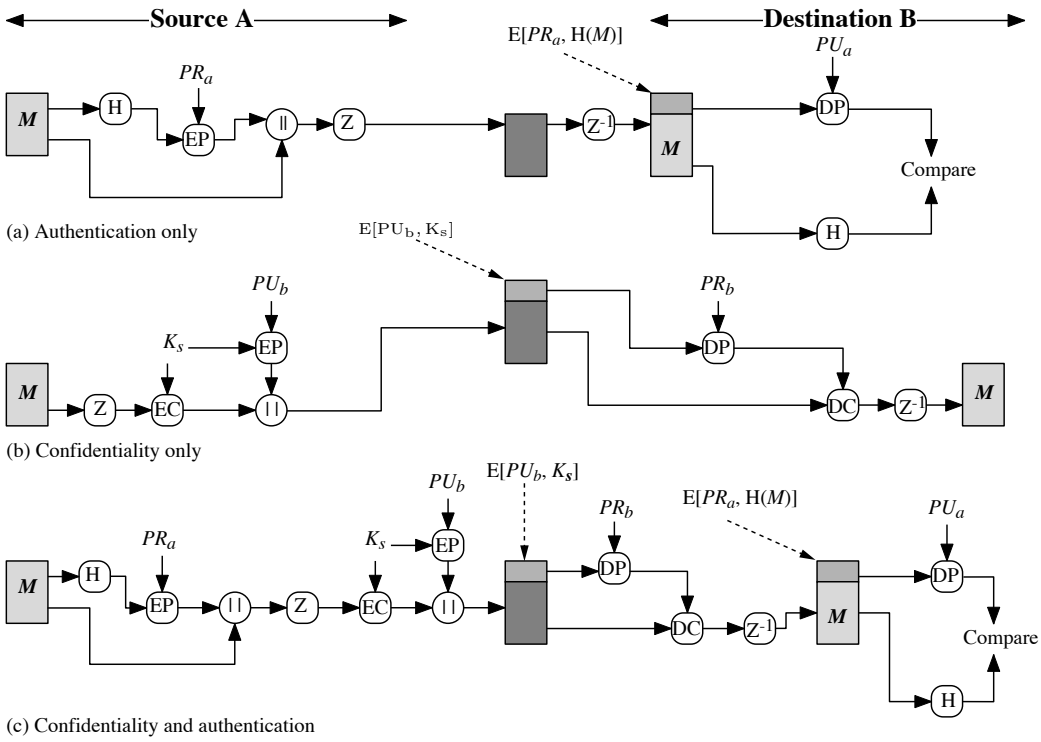
   Soluzione.

   Plaintext: `GUARDIAIMPERIALE`
   Ciphertext: `IMECFAETOHICKSPP`
   Chiave: 2 18 4 11

2. ***Message Encryption***

Si scrivano nei riquadri bianchi le proprietà di sicurezza assicurate da ciascuno dei seguenti schemi crittografici.

Soluzione.



3. ***Crittografia a chiave pubblica I***

Si illustri l'interazione tra PC e smartcard nelle seguenti attività:

1. *Firma di un documento*
2. *Verifica della firma di un documento*

Soluzione.

1. Il PC calcola e invia alla smartcard lo hash del documento da firmare. La smartcard cifra il valore ricevuto con la chiave privata in essa memorizzata e invia al PC il risultato. In nessun caso la smartcard trasmette verso l'esterno la chiave privata in essa memorizzata.

2. La smartcart non gioca alcun ruolo in quanto non è necessario utilizzare la chiave privata del possessore. Per la verifica della firma serve un certificato digitale di colui che ha firmato il documento.

4. ***Crittografia a chiave pubblica II***

Si consideri l'algoritmo RSA con $p = 7$, $q = 13$ e $e = 23$.

- *Si calcoli il testo cifrato* C *corrispondente al testo in chiaro* $M = 51$.
- *Si calcoli la chiave di decifrazione* (d, n).
- *Si verifichi che decifrando* C *con* (d, n) *si riottiene* M.

Si giustifichino le risposte date scrivendo tutti i calcoli intermedi.

Si utilizzino le seguenti tabulazioni (ovviamente parziali) delle funzioni di esponenziazione modulare e dell'inverso moltiplicativo modulo n*:*

a	b	n	$a^b \mod n$
19	82	11	9
51	91	23	10
91	23	51	31
99	12	91	1
25	47	91	51
51	23	91	25
47	25	91	47
99	13	15	9

x	y	$x^{-1} \mod y$
72	23	8
21	91	87
21	73	7
7	13	2
13	7	6
23	72	47
23	91	4
21	72	7
91	23	22
91	23	22

Soluzione. Siccome $p = 7$, $q = 13$, allora $n = pq = 91$. Quindi $C = M^e \mod n = 51^{23} \mod 91 = 25$.
La chiave di decifrazione è data da (d, n) dove $d = e^{-1} \mod \Phi(n) = 23^{-1} \mod 72 = 47$.
Infatti $\Phi(n) = (p-1)(q-1) = 6 * 12 = 72$.
Infine verifichiamo che $C^d \mod n = 25^{47} \mod 91 = 51 = M$.

5. ***Protocolli di Sicurezza***

Si consideri il seguente protocollo P_1 per la creazione di una chiave condivisa tra due agenti A e B:

1. $A \rightarrow B : \{A, Na\}_{Kb}$
2. $B \rightarrow A : \{B, Nb\}_{Ka}$
3. $A \rightarrow B : \{zero, Msg\}_{Na \oplus Nb}$
4. $B \rightarrow A : \{one, Msg\}_{Na \oplus Nb}$

dove $zero$ e one sono identificatori distinti e $Na \oplus Nb$ è lo XOR bit a bit di Na e Nb.

(a) Si descrivano i singoli passi del protocollo e le proprietà di sicurezza per il quale è stato presumibilmente progettato.

Soluzione. Il protocollo dovrebbe garantire:

1. la mutua autenticazione tra A e B
2. lo scambio confidenziale di una nuova chiave $Na \oplus Nb$ e di Msg.

(b) Si discuta se il protocollo garantisce o meno le proprietà di sicurezza indicate nella risposta alla domanda (a). Si supponga che la crittografia sia perfetta (ovvero non è soggetta ad attacchi di crittoanalisi).

Soluzione. Il protocollo non è vulnerabile. La presenza dell'identificatore del mittente nei messaggi inviati ai passi 1 e 2 rende difficile la realizzazione di *replay attacks*. La presenza degli identificatori $zero$ e one nei messaggi inviati ai passi 3 e 4 rende difficile la realizzazione di *reflection attacks*.

6. ***Controllo degli Accessi***

Si consideri il modello MAC di Bell-La Padula e si indichino i permessi concessi ad un utente con security label *(secret, {personnel, design, assistance}) relativamente a documenti classificati nel seguente modo:*

1. *(top secret, {design}):*
2. *(top secret, {personnel, production, design, assistance}):*
3. *(secret, {personnel, assistance}):*
4. *(secret, {production, design}):*
5. *(secret, {}):*
6. *(confidential, {personnel, assistance}):*
7. *(confidential, {production, design}):*
8. *(confidential, {}):*

Soluzione. Ricordiamo che (r_2, c_2) domina (r_1, c_1) (in simboli, $(r_1, c_1) \leq (r_2, c_2)$ se e solo se $r_1 \leq r_2 \wedge c_1 \subseteq c_2$ e che gli accessi nel modello di Bell-LaPadula sono governati dai seguenti due principi:

- **No Read-Up** (detta anche **Simple Security Property**): Un subject con clearance x_s può leggere informazione relativa ad una risorsa con security label x_o solo se x_s domina x_o.
- **No Write-Down** (detta anche ***-Property**): Un subject con clearance x_s può scrivere informazione su un oggetto con security label x_o solo se x_o domina x_s.

Dunque le risposte sono:

1. (top secret, {design}): nessun diritto
2. (top secret, {personnel, production, design, assistance}): sola scrittura
3. (secret, {personnel, assistance}): sola lettura
4. (secret, {production, design}): nessun diritto
5. (secret, {}): sola lettura
6. (confidential, {personnel, assistance}): sola lettura
7. (confidential, {production, design}): nessun diritto
8. (confidential, {}): sola lettura