CORSO DI SICUREZZA INFORMATICA 1 (A.A. 2008/2009)

Prof. A. Armando

(10 Luglio 2009)

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

Nome e Cognome: _____

Matricola: _____

---

1. ***Crittografia a Chiave Pubblica***

   Si consideri lo schema di Diffie-Hellman dove $q = 11$ e $\alpha = 2$.

   (a) Se A ha chiave pubblica $Y_A = 9$, qual è la chiave privata di A?

   Soluzione.

   $$X_A = 6$$

   (b) Se B ha chiave pubblica $Y_B = 3$, qual è la chiave segreta K?

   Soluzione.

   $$K = 3$$

2. ***Crittografia***

Un sistema consente all'utente di scegliere una password con una lunghezza minima di un carattere e massima di 8 caratteri. Si assuma che sia possibile testare 10.000 password al secondo. L'amministratore di sistema vuole disabilitare le password non appena si abbia la probabilità 0.1 che sia stata scoperta.

Si determini il tempo medio dopo con cui questa probabilità viene raggiunta nel caso in cui i caratteri con cui sono formate le password siano:

(a) *Caratteri ASCII con codici da 1 to 127, estremi inclusi.*

Soluzione.

(b) *Caratteri alfanumerici (da 'A' a 'Z,' da 'a' a 'z,' e da '0' a '9').*

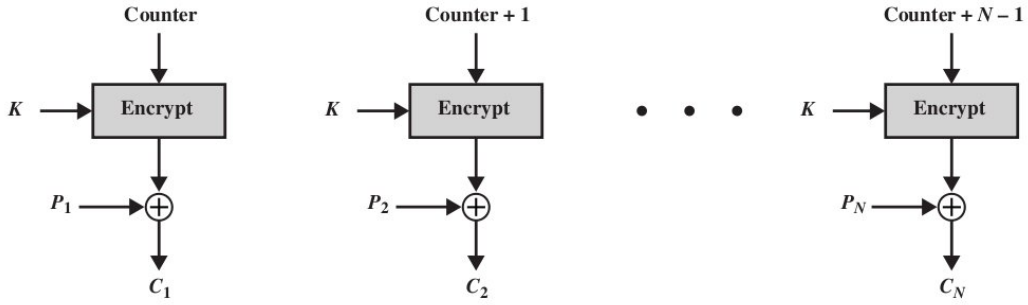
Soluzione.

(c) *Numeri (da '0' a '9').*

Soluzione.

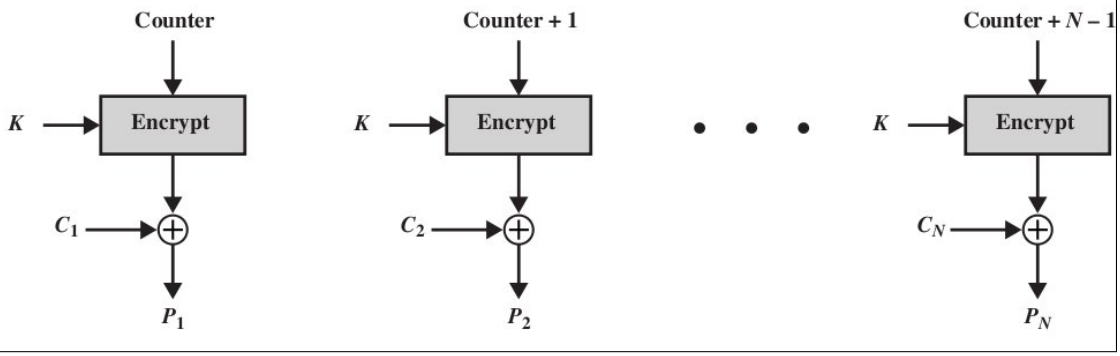
3. ***Crittografia***

Il seguente schema crittografico per block encription. ***Counter*** *è una sequenza di bit arbritraria della stessa linghezza* b *dei blocchi di dati e l'operazione di somma è da intendersi modulo* 2^b.



(a) *Si disegni il corrispondente schema crittografico da usarsi in fase di decifratura.*

Soluzione.



(b) *Tale schema crittografico si presta a implementazioni più o meno efficienti rispetto allo schema CBC visto a lezione? Si giustifichi la risposta data.*

Soluzione.
A differenza dello CBC lo schema è altamente parallelizzabile e la cifrature possono essere precomputate.

4. ***Protocolli di Sicurezza***

Si consideri il seguente protocollo per l'autenticazione di due agenti in possesso di una chiave simmetrica condivisa K.

$$\begin{array}{ll} 1. & A \to B: \quad N \oplus K \\ 2. & B \to A: \quad N \end{array}$$

Il primo agente (A) genera una nonce N della stessa lunghezza di K, la mette in $\oplus$ con K e la invia al secondo agente (B). Quando B riceve il messaggio da A, lo mette in $\oplus$ con la chiave K e manda la stringa di bit risultante indietro ad A. Se la stringa di bit ricevuta da A coincide con la nonce generata inizialmente, allora A può concludere di aver autenticato B.

(a) *Si indichino almeno due proprietà che sono fondamentali per la sicurezza di un protocollo di autenticazione di questo tipo.*

Soluzione.

- Autenticazione di B nei confronti di A
- Segretezza della chiave K

(b) *Si discuta se le proprietà indicate sono soddisfatte dal protocollo in questione.*

Soluzione.
La chiave K viene compromessa. Infatti, mettendo in $\oplus$ i messaggi scambiati durante l'esecuzione del protocollo si ottiene la chiave K.

5. ***Crittografia a Chiave Pubblica***

Rispondere alle seguenti domande, giutificando le risposte date:

(a) *Dire quali dei seguenti oggetti digitali può essere utilizzato come certificato digitale per un sito web:*

Soluzione.

- ☐ un documento contenente il nome del sito, la sua chiave privata, il tutto cifrato con la chiave pubblica di un'Autorità di Certificazione.
- ☐ un documento contenente il nome del sito, la sua chiave pubblica, il tutto cifrato con la chiave pubblica di un'Autorità di Certificazione.
- ☐ un documento contenente il nome del sito, la sua chiave privata, il tutto cifrato con la chiave privata di un'Autorità di Certificazione.
- ☑ un documento contenente il nome del sito, la sua chiave pubblica, il tutto cifrato con la chiave privata di un'Autorità di Certificazione.

(b) *Alice deve inviare un file M di grosse dimensioni a Bob (ad esempio un filmato di qualche Gbyte) in modo tale che Bob sia certo dell'integrità della trasmissione. Quali tra le seguenti procedure sono adeguate allo scopo?*

Soluzione.

- ☐ Alice calcola ed invia a Bob: M e la fingerprint di M cifrata con la chiave pubblica di Bob.
- ☐ Alice calcola ed invia a Bob: M e la fingerprint di M cifrata con la chiave privata di Bob.
- ☑ Alice calcola ed invia a Bob: M e la fingerprint di M cifrata con la propria chiave privata.
- ☐ Alice calcola ed invia a Bob: M e la fingerprint di M cifrata con la propria chiave pubblica.

(c) *Supponete di essere proprietari di una azienda e che un vostro cliente vi invii un contratto firmato digitalmente in cui si impegna a pagare una fornitura di beni da voi prodotti ad una somma stabilita a 120 giorni dalla consegna dei beni stessi. La verifica della firma digitale va fatta:*

Soluzione.

- ☐ Solo in caso di contestazione.
- ☑ Prima di effettuare la fornitura.
- ☐ Anche dopo la consegna della fornitura di beni, ma entro i 120 giorni.

6. ***Controllo degli Accessi I***

Si classifichino le seguenti situazioni come esempi di poliche di controllo degli accessi ***mandatory***, ***discrezionali***, *o la loro combinazione. Si giustifichino le risposte date.*

(a) *I meccanimi di controllo degli accessi del sistema operativo UNIX*

Soluzione. Discrezionale

(b) *Il caveau di una banca in cui solo i membri del consiglio di amministrazione possono entrare*

Soluzione. Mandatory

(c) *L'archivio di un ospedale comune dova la cartella clinica di un paziente P può essere consultato per condurre analisi statistiche se P ha dato un permesso scritto che autorizzi questa operazione.*

Soluzione. Sia discrezionale che mandatory.

7. ***Controllo degli Accessi II***

Si consideri il seguente insieme di diritti {R,W,X,A,L,M,Own}*, dove* A*,* L *e* M *stanno per* Append, List *e* Modify*.*

(a) Utilizzando la sintassi del modello di Harrison-Ruzzo-Ullman, si scriva il comando per create(s, o)*, con il quale* s *viene creata la risorsa* o *e viene dato ad* s *il solo diritto di possesso (*Own*).*

Soluzione.

```
command create(s,o)
 create object o
 enter Own into M(s,o)
end
```

(b) Utilizzando la sintassi del modello di Harrison-Ruzzo-Ullman, si scriva il comando per transfer.write(s_1, s_2, o)*, con il quale se* s_1 *ha il diritto di scrittura su* o *allora lo trasferisce (perdendolo) a* s_2*.*

Soluzione.

```
command tranfer.write(s1,s2,o)
 if W in M(s1,o)
 then enter W into M(s2,o)
      delete W from M(s1,o)
end
```