

SICUREZZA DELLE RETI
Prof. Maurizio Dècina
Recupero del 29-7-2003
(due ore di tempo)

Quesito 1

Sia dato un alfabeto composto dai simboli esadecimali (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F). Si impieghi un algoritmo di cifratura a catena del tipo CBC (Cipher Block Chaining), ove:

1) $C_i = E_k(C_{i-1} \oplus P_i)$ per $i=2, 3, \dots, n$; mentre per $i=1$ si pone $C_0 = IV$ (Initialization Vector).

Si scelga $n=3$ e $IV=1010$.

L'algoritmo di cifratura a chiave segreta è quello del cifrario 'affine', ove:

2) $E_k(X) = (aX + b) \bmod 16$, ove $K=(a,b)$.

Si scelga $a=5$, e $b=3$.

- a) Descrivere la funzione di decifratura da eseguire su CBC con schemi a blocchi e con le equazioni inverse delle 1).
- b) Scrivere la funzione di decifratura inversa della 2) inclusi i suoi parametri numerici.
- c) Qual'è la complessità dell'attacco all'algoritmo 'CBC-affine' qui illustrato?
- complessità intesa come numero delle possibili diverse 'chiavi' -
- d) Dato il messaggio testuale in chiaro $P_1 P_2 P_3 = C F O$; determinare il messaggio cifrato $C_1 C_2 C_3$.
- e) Dato il messaggio cifrato $C_1 C_2 C_3$, decifrare per riottenere il messaggio in chiaro $P_1 P_2 P_3$.

Quesito n.2

Bob adotta lo schema di firma di ElGamal e sceglie $p = 53$. Pubblica quindi i valori:

$p = 53$

$\alpha = 5$

$\beta = ?$

e tiene segreti i valori:

$a = 19$

$k = 1$.

- a) Enunciare le ipotesi dello schema di firma di ElGamal per i parametri (p, a, k) .
 - i. Quanti e quali sono i possibili simboli P che si possono firmare con questo schema?
 - ii. Quanti e quali sono i possibili valori di k ?
- b) Dire quanti sono gli elementi primitivi $\in Z_p^*$.
- c) Verificare che $\alpha = 5$ è un elemento primitivo di Z_p^* .
- d) Determinare il valore di β .
- e) Qual'è la firma del messaggio in chiaro $P = 42$?
- f) Verificare la firma determinata al punto precedente

Quesito 3

Si illustri la Versione 5 del protocollo 'Kerberos'.

- a) Applicazioni 'client-server' tra 'realm' multipli di Kerberos.
- b) Messaggi e funzioni dei messaggi:
 - i. Messaggi tra 'client' e 'server di autenticazione'
 1. 'ticket di autenticazione'.
 - ii. Messaggi tra 'client' e 'server di emissione biglietti'
 1. 'autenticatore' e 'ticket di servizio'.
 - iii. Messaggi tra 'client' e 'server delle applicazioni'
 1. 'autenticatore'.
- c) Funzioni associate ai 'flag' dei 'ticket di servizio'

Quesito 4

Si illustrino i meccanismi di sicurezza adottati nel protocollo IPsec per quanto riguarda:

- a) Associazioni di sicurezza e distribuzione delle chiavi crittografiche.
- b) Integrità dei pacchetti IP
 - i. Header AH.
 - ii. Metodologia di autenticazione della sorgente e del messaggio.
 - iii. Algoritmi di crittografia.
- c) Cifratura dei pacchetti IP
 - i. Header ESP.
 - ii. Metodologia di cifratura e di autenticazione della sorgente e del messaggio.
 - iii. Algoritmi di crittografia.

Quesito 1	7.5
Quesito 2	7.5
Quesito 3	7.5
Quesito 4	7.5