LAUREA SPECIALISTICA IN INGEGNERIA INFORMATICA

SICUREZZA NELLE RETI

Appello del 17 Febbraio 2005

Nome e Cognome _____ **Matricola** _____

ESERCIZIO 1 — PUNTI: 14 (3, 3, 2, 3, 3)

Con riferimento al sistema di crittografia One-time Pad, il candidato, con precisione matematica e proprietà di linguaggio,

1. descriva gli algoritmi di generazione della chiave, di cifratura e di decifratura;
2. specifichi le condizioni sotto le quali il cifrario è perfetto;
3. illustri le implicazioni pratiche di tali condizioni.

Siano P = "MARIOROSSI0850EURO", K = "5RTIOX1LQB39DEMZAN",

4. si determini C sapendo
   - che $C[i]$, $P[i]$ e $K[i]$ sono la rappresentazione dell'i-esimo carattere di C, P e K, rispettivamente;
   - che il generico carattere è rappresentato dall'intero che esprime la sua posizione, a partire da zero, nell'alfabeto $\mathcal{A}$ = {'A', 'B', …, 'Z', '0', '1', …, '9'};
   - che $C[i] = P[i] \oplus K[i]$ per ogni carattere di P.
5. si determini la probabilità che un avversario, operando sul solo testo cifrato, riesca ad incrementare la cifra più significativa dell'importo sapendo che tale importo è minore di 1000 euro.

SOLUZIONE.

Punti 1–3. Vedere il materiale didattico.

Punto 4. Eseguire le somme modulo 31.[1]

Punto 5. L'avversario ha la certezza del successo del suo attacco. Sapendo che l'importo è minore di 1000 euro, l'avversario sa che la cifra più significativa è rappresentata dal carattere p = '0'. Conoscendo il carattere c del crittogramma corrispondente a p ('Q'), l'avversario è in grado di determinare il carattere k della chiave associato a p e c come $p \oplus c$. Tale carattere è '3'. A questo punto l'avversario può calcolare il carattere c' da sostituire nel crittogramma al posto di 'Q', $c' = k \oplus$ '1' = 'R'.

Più semplicemente si poteva osservare che $c' = p \oplus 1 \oplus k = c \oplus 1$.

ESERCIZIO 2 — PUNTI: 8 (4, 4)

1. Bob riceve il messaggio $\langle$Alice, m, Π, $\sigma\rangle$ e verifica con successo la firma digitale σ di m per mezzo della chiave pubblica Π. Indicare quale delle seguenti conclusioni Bob può correttamente trarre, motivando la scelta:

[1] Oppure modulo 36 se si considera l'alfabeto inglese. Noi consideriamo quello italiano.

a) Il messaggio *m* è stato firmato con la chiave privata di Alice;
b) Il messaggio *m* è stato firmato con la chiave privata corrispondente a Π;
c) Il messaggio *m* è stato firmato da Alice.

2. Sia *T* un'autorità di certificazione di fiducia di Bob, di cui Bob conosce la chiave pubblica Π_T. Sia inoltre X(*T*, *A*) un certificato rilasciato da *T* ad *Alice*. Bob riceve il messaggio $\langle A, m, \sigma, X(T, A)\rangle$ e verifica con successo le firme digitali. Quale delle precedenti conclusioni Bob può adesso correttamente trarre? Motivare la scelta.

SOLUZIONE.

Quesito 1. Bob può giungere alla conclusione b.

Quesito 2. Bob può giungere alla conclusione a.

ESERCIZIO 3 **PUNTI: 10 (3, 4, 3)**

Con riferimento a Kerberos 5, il candidato

1. illustri il protocollo semplificato;
2. lo analizzi con la logica BAN;
3. discuta l'impatto che il *ticket lifetime* e l'*authenticator lifetime* hanno sulla sicurezza del protocollo.

SOLUZIONE. Vedere il materiale didattico.

LAUREA SPECIALISTICA IN INGEGNERIA INFORMATICA

SICUREZZA NELLE RETI

Appello del 31 Gennaio 2006

SOLUZIONE

ESERCIZIO 1

ESERCIZIO 2

ESERCIZIO 3