Corso di Sicurezza nelle reti
a.a. 2010/2011

Raccolta di alcuni quesiti sulla prima parte del corso

1) Si consideri un semplice cifrario a sostituzione con shift (tipo cifrario di Cesare), con un alfabeto di N caratteri (con N=21 o 26 a scelta), con chiave K=4. Si cripti la stringa "SEGRETO"

Plain text	*Cipher text*
SEGRETO	

2) Si indichi lo schema di un singolo round del DES$^-$ (o anche di un generico cifrario di Feistel), senza entrare nel dettaglio della funzione di mangle f(·).

3) Dato un algoritmo $E_K(\cdot)$ di crittografia a blocchi di lunghezza q, si descriva lo schema di codifica di tipo CBC (Cipher Block Chaining) di un messaggio m di lunghezza L>q (si supponga per semplicità L=n q).

4) Si consideri un algoritmo $E_k(\cdot)$ di crittografia a blocchi di dimensione 4 bit. Supponendo che data una chiave segreta K la tabella di codifica di $E_k(\cdot)$ sia la quella riportata a lato, si chiede di criptare in modalità CBC con IV=0000 il seguente messaggio in chiaro:

m= 1100 1010 0010 1101

plaintext	*ciphertext*
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

5) Si consideri il seguente messaggio in chiaro:

m = 1100 0000 1100 0000

che viene inviato criptato utilizzando lo stesso algoritmo di crittografia simmetrica a blocchi di dimensione 4bit $E_k(\cdot)$ e stessa chiave K dell'esercizio precedente (stessa tabella di sostituzione/codifica) in modalità OFB con IV=0001, ottenendo:

c = 1000 0010 0001 1001 (IV=0001)

Si chiede di: indicare come deve essere modificato tale messaggio cifrato in modo che decifrandolo si ottenga:

m'= 1100 0000 1001 0000

6) Indicare lo schema del HMAC in funzione di un algoritmo di hash H(.), e calcolare il numero di passate che devono essere svolte con H durante il calcolo dell'HMAC di un messaggio m lungo N.M dove M è la dimensione di blocco che H elabora in una singola passata (e.g. M=512bit nel caso di MD5 e SHA1).

Schema dell'HMAC

Numero di passate necessarie per calcolare l'HMAC di un messaggio lungo N·M dove M è la dimensione di blocco di H:	

7) Costruire uno schema di crittografia simmetrica per criptare messaggi m di qualsiasi lunghezza tramite chiave segreta K, basato su algoritmo di crittografia a blocchi $E_K()$ (e.g. AES) ma SENZA effetto valanga, cioè in modo che la modifica di un bit del testo cifrato abbia effetto su un solo bit del testo in chiaro (Suggerimento, nello schema utilizzare anche l'operazione XOR).

8) Si supponga di voler inviare in modo sicuro un messaggio *m* da A a B, garantendo SOLO la confidenzialità dei dati inviati. Per la cifratura del messaggio si utilizzi un algoritmo di crittografia simmetrica. Indicare schematicamente quali funzioni possono essere svolte in fase di invio/ricezione, supponendo che A e B condividano tra loro solo le rispettive chiavi RSA pubbliche KU_A e KU_B (si indichino con KR_A e KR_B le corrispondenti chiavi private).

Invio	Ricezione

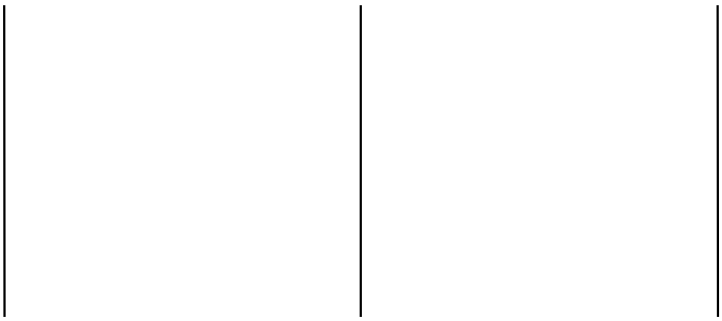
9) Si supponga di voler inviare in modo sicuro un messaggio *m* da A a B, garantendo SOLO l'autenticità/integrità dei dati inviati. Indicare schematicamente quale funzioni possono essere svolte in fase di invio/ricezione, supponendo che A e B condividano una chiave segreta K_{AB}, e che dispongano solo di un algoritmo di hash H().

Invio	Ricezione

10) Indicare un possibile schema sicuro di autenticazione tra Alice (supplicant) e Bob (authenticator), nell'ipotesi che Alice e Bob condividano le rispettive chiavi RSA pubbliche KU_A e KU_B (si indichino con KR_A e KR_B le corrispondenti chiavi private).

11) Indicare un possibile schema sicuro di mutua autenticazione tra due utenti Alice e Bob, basato sull'uso di una funzione hash H(·) e su un segreto condiviso K_{AB}.

12) Si consideri uno schema di scambio di chiavi tra A e B di tipo Diffie-Hellman, e si indichi come questo può essere attaccato con successo da una terza parte C.



13) Perché il seguente schema di distribuzione di chiave di sessione Ks tramite crittografia simmetrica non è sicuro? (si è indicato con Ka e Kb le chiavi segrete condivise rispettivamente tra KDC e A, e KDC e B; con Ks la chiave di sessione)

A → KDC: IDa, IDb
KDC→ A: IDb, Ks
A → B: IDa, Ks

b) E il seguente?

A → KDC: ID_A, ID_B
KDC→ A: IDb, {Ks}Ka ,{Ks}Kb
A → B: IDa, {Ks}Kb

c) Come è possibile migliorare il precedente schema?

14) Nell'ipotesi che date tre entità A, B e C:

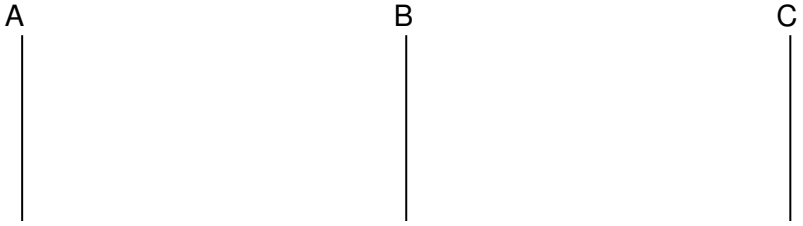
i) A possieda una coppia di chiavi privata/pubblica KR_A e KU_A;

ii) C possieda la chiave pubblica di A, KU_A;

iii) B e C condividano una chiave segreta K_{BC};

iv) B e C non dispongano di alcun canale di comunicazione tra loro.

Si chiede di indicare un possibile schema di comunicazione tramite il quale sia possibile instaurare una associazione sicura tra A e B (K_{AB}).



15) Nell'ipotesi che A possieda i seguenti certificati digitali: $cert_{A|CA3}$, $cert_{CA3|CA2}$, $cert_{CA2|CA1}$, e $cert_{CA1|CA1}$ (dove è indicato con $cert_{X|Y}$ il certificato di X firmato da Y), indicare cosa è necessario che A invii a B in modo tale che B possa comunicare in modo sicuro con A, nei seguenti casi:

B possiede:	A deve inviare a B:
$cert_{CA1\|CA1}$	
$cert_{A\|CA3}$	
$cert_{CA2\|CA1}$	
$cert_{CA1\|CA1}$, $cert_{A\|CA3}$	

16) Se A possiede $cert_{A|B}$ e $cert_{B|C}$ (dove si è indicato con $cert_{X|Y}$ il certificato di X firmato da Y), mentre D possiede $cert_{D|E}$, indicare:

a) cosa deve possedere A per autenticare D? indicare anche un possibile schema di autenticazione.

b) cosa deve possedere D per autenticare A? indicare anche un possibile schema di autenticazione.

17) Si costruisca una coppia di chiavi privata/pubblica per RSA, utilizzando come coppia di numeri primi *p* e *q* i seguenti valori: p=3, q=11. Con tale chiavi si cripti il messaggio m=2.

18) Si faccia un esempio di creazione di chiave condivisa tra A e B con Diffie-Hellman, utilizzando per il generatore g e il numero primo p i seguenti valori: g=2, p=11.

19) Tramite l'algoritmo di Euclide determinare il massimo comune divisore gcd(,) tra:
a) 36, 15
b) 47, 20
c) 43, 35

20) Determinare λ , $\mu \in \mathbb{Z}$ tali che$25\,\lambda + 32\,\mu = 1$, per mezzo dell'Algoritmo di Euclide esteso, ed utilizzare il risultato ottenuto per risolvere l'equazione $25\,x \equiv 4 \bmod 32$

21) Si costruisca una coppia di chiavi privata/pubblica per RSA, utilizzando come coppia di numeri primi *p* e *q* i seguenti valori: p=7, q=11 e come chiave pubblica KU=<e,n> con e=13. Con tale chiavi si decripti il messaggio c=2.