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

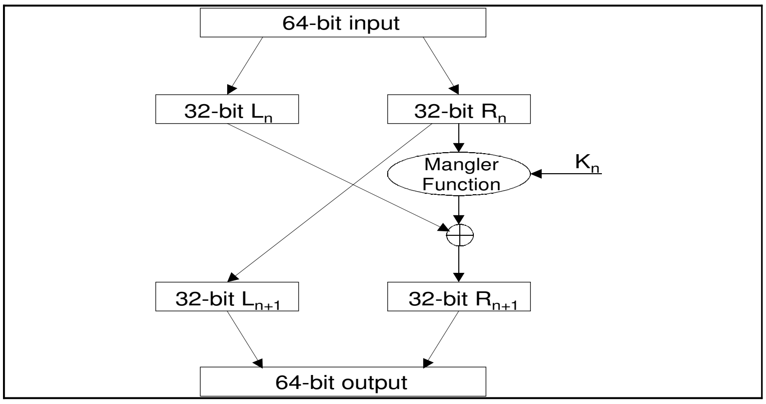
Soluzione dei quesiti sulla prima parte del corso

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"

SOLUZIONE
Nel caso si consideri un alfabeto di 21 caratteri, c = $E_k(m)$ = E_4("SEGRETO") = "ZIMVIAS"
Nel caso si consideri invece un alfabeto di 26 caratteri, c = "WIKVIXS"

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(·).

SOLUZIONE



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).

SOLUZIONE
$m=m1||m2|| \ldots ||m_n$
$c=IV||c1||c2|| \ldots ||c_n$

con:
$c_0=IV$
$c_i=Ek(m_i \oplus c_{i-1})$

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

SOLUZIONE

c= `0101 0111 1111 1101` (iv=0000)

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`

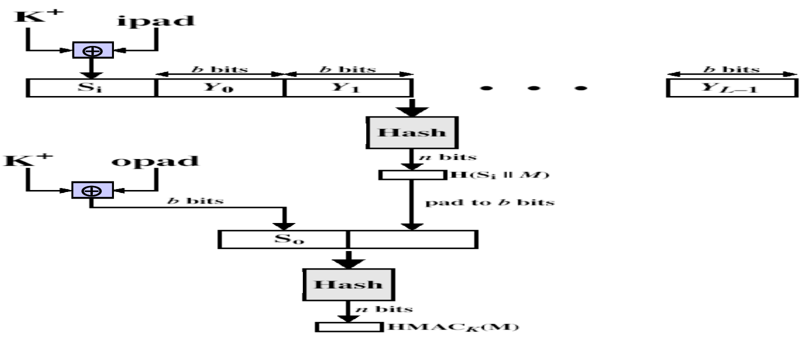
SOLUZIONE

c'= `1000 0010 0100 1001 (iv=0001)`

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).**

SOLUZIONE

Schema dell'HMAC



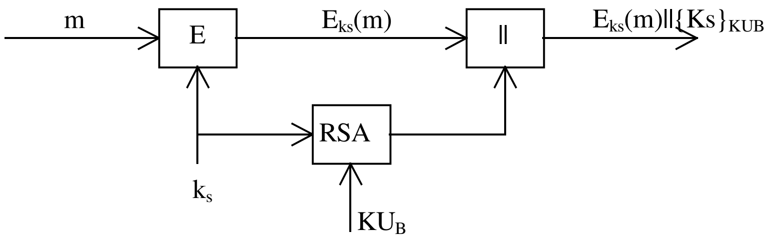
Numero di passate necessarie per calcolare l'HMAC di un messaggio lungo N·M dove M è la dimensione di blocco di H:	N+3

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).

SOLUZIONE
$m=m1||m2|| \ldots ||m_n$
$c=IV||c1||c2|| \ldots ||c_n$
$c_i=m_i \oplus o_i$
con:
$o_i= Ek(o_{i-1})=AES(k,o_{i-1})$
$o_0=IV$

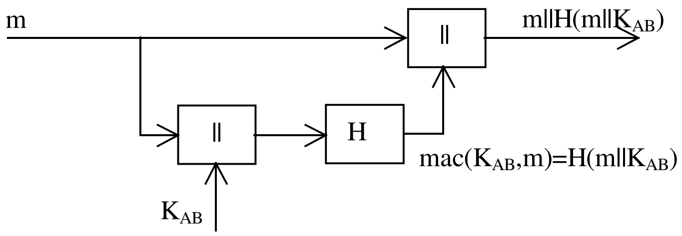
8) Si supponga di voler inviare in modo sicuro un messaggio *m* da A a B, garantendo SOLO la confidenzialità dei dati inviati. Per la cifratura del messaggio si utilizzi un algoritmo di crittografia simmetrica. Indicare schematicamente quale funzioni possono essere svolte in fase di invio/ricezione, 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).

SOLUZIONE



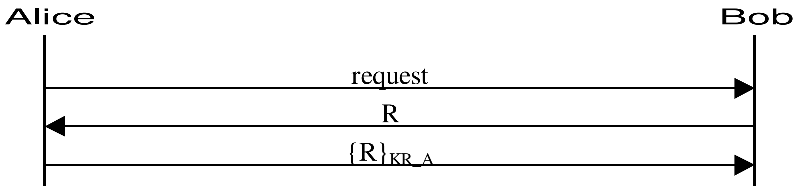
9) Si supponga di voler inviare in modo sicuro un messaggio *m* da A a B, garantendo SOLO l'autenticità/integrità dei dati inviati. Indicare schematicamente quale funzioni possono essere svolte in fase di invio/ricezione, supponendo che A e B condividano una chiave segreta K_{AB}, e che dispongano solo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

SOLUZIONE

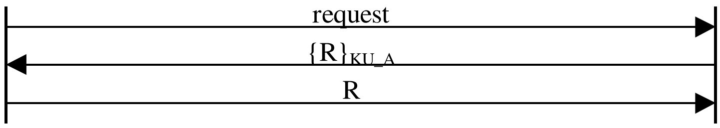


10) Indicare un possibile schema sicuro di autenticazione tra Alice (supplicant) e Bob (authenticator), nell'ipotesi che Alice e Bob condividano le rispettive chiavi RSA pubbliche KU_A e KU_B (si indichino con KR_A e KR_B le corrispondenti chiavi private).

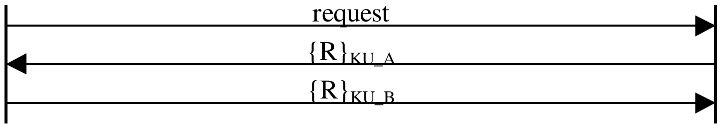
SOLUZIONE



oppure:

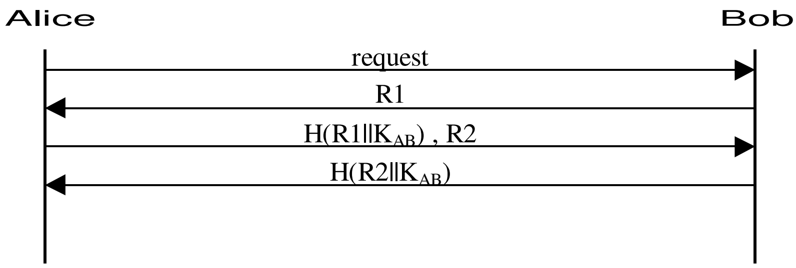


oppure:



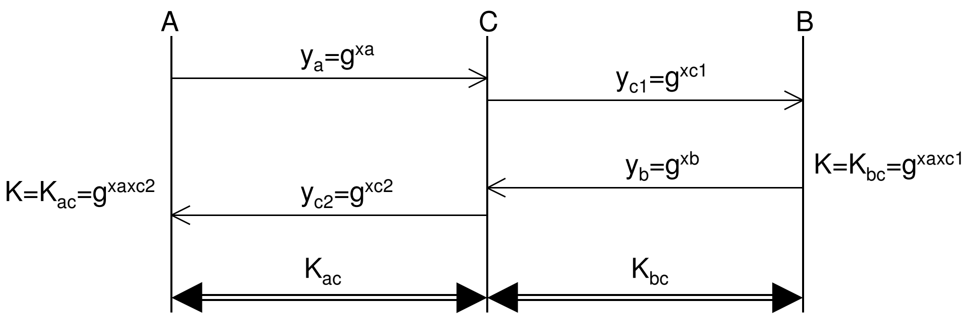
11) Indicare un possibile schema sicuro di mutua autenticazione tra due utenti Alice e Bob, basato sull'uso di una funzione hash H(·) e su un segreto condiviso K_{AB}.

SOLUZIONE



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.

SOLUZIONE



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?

SOLUZIONE
a) A riceve dal KDC la chiave di sessione Ks in chiaro, chiunque che può intercettare la comunicazione può ottenere Ks

b) B non ha la prova che la chiave ricevuta è condivisa con A e di parlare proprio con A; ad esempio un intruso C capace di intercettare e modificare la comunicazione tra A e B può ingannare B facendogli credere di dialogare con D (senza però riuscire a decriptate la comunicazione) in questo modo:

A $\rightarrow$ KDC: IDa,IDb
KDC $\rightarrow$ A: IDb,$\{Ks\}_{Ka}$,$\{Ks\}_{Kb}$
A $\rightarrow$ C: IDa, $\{Ks\}_{Kb}$
C $\rightarrow$ B: IDd, $\{Ks\}_{Kb}$

Inoltre se l'intruso è utente valido del KDC, che ha precedentemente parlato con B può ottenere dal KDC una chiave Ks1valida per parlare con A (caso 1) o con B (caso 2) e sostituire il messaggio inviato dal KDC ad A con IDb,$\{Ks1\}_{Ka}$,$\{Ks1\}_{Kc}$ (nel caso 1), oppure sostituire con IDb,$\{Ks1\}_{Kc}$,$\{Ks1\}_{Kb}$ (nel caso 2); nel primo caso è in grado di decriptare i messaggi inviati da A a B, mentre nel secondo quelli inviati da C ad A.

c) uno schema più sicuro è il seguente (Needham & Schroeder):

A $\rightarrow$ KDC: IDa,IDb,Na
KDC $\rightarrow$ A: $\{Ks,IDb,Na,\{Ks,IDa\}Kb\}_{Ka}$
A $\rightarrow$ B: $\{Ks,IDa\}_{Kb}$
B $\rightarrow$ A: $\{Nb\}_{Ks}$
A $\rightarrow$ B: $\{Nb-1\}_{Ks}$

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;

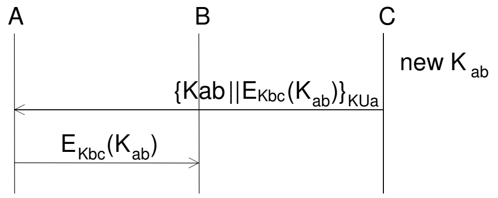
ii) C possieda la chiave pubblica di A, KU_A;

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}).

SOLUZIONE
Un possibile schema che permette ad A e B di ottenere una chiave condivisa Kab è il seguente:



cioè:

C $\rightarrow$ A: $\{Kab, \{Kab\}_{Kbc}\}_{KUa}$
A $\rightarrow$ B: $\{Kab\}_{Kbc}$

Volendo proteggere lo scambio di chiave anche da attacchi di tipo replay e/o sostituzione si può ricorrere ad uno schema tipo KDC (Needham & Schroeder) dove però viene usata la chiave pubblica di A al posto di quella condivisa tra A e C (KDC):

A $\rightarrow$ C: IDa,IDb,Na
C $\rightarrow$ A: $\{Kab,IDb,Na,\{Kab,IDa\}_{Kbc}\}_{KUa}$
A $\rightarrow$ B: $\{Kab,IDa\}_{Kbc}$
B $\rightarrow$ A: $\{Nb\}_{Kab}$
A $\rightarrow$ B: $\{Nb-1\}_{Kab}$

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:

SOLUZIONE

B possiede:	A deve inviare a B:
$cert_{CA1|CA1}$	$cert_{A|CA3}$, $cert_{CA3|CA2}$, $cert_{CA2|CA1}$
$cert_{A|CA3}$	nulla (nessun certificato, solo l'identità di A)
$cert_{CA2|CA1}$	$cert_{A|CA3}$, $cert_{CA3|CA2}$
$cert_{CA1|CA1}$, $cert_{A|CA3}$	nulla (nessun certificato, solo l'identità di A)

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.

SOLUZIONE
a) La chiave pubblica di D (o un certificato di D),
oppure la chiave pubblica di E (o un certificato di E)

b) La chiave pubblica di A (o un certificato di A),
oppure la chiave pubblica di B (o un certificato di B),
oppure la chiave pubblica di C (o un certificato di C).

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.

SOLUZIONE
n=pq=33
$\phi(n)=(p-1)(q-1)=20$
possibili candidati alla coppia e,d sono: 1,3,7,9,11,13,17,19
se si sceglie *e*=7, si trova che il moltiplicativo inverso di *e* modulo $\phi(n)$ è *d*=3; infatti ed=1 mod 20
e e *d* possono essere usate rispettivamente come chiave pubblica e privata per cifrare decifrare m; quidi:
$c=E(m)=2^7$ mod 33=29
si può verificare che:
$m=D(c)=29^3$ mod 33=((29x29) mod 33) mod 33)=16x29 mod 33=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.

SOLUZIONE
Supponendo che A scelga il segreto $x_a=5$, mentre B scelga il segreto $x_b=3$, si ha:
A invia a B ya=g^{xa}mod p=10
B invia ad A ya=g^{xb}mod p=8
dati ya e xb, B costruisce: Kba=ya^{xb} mod p=10^3=100x10=1x10=10
dati yb e xa, A costruisce Kab= yb^{xa} mod p=$8^5=(8^2)^2x8=2^2x8$=4x8=10
giustamente si ha Kab=Kba

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

SOLUZIONE
a) gcd(36,15)=(36,15)=(15,6)=(6,3)=3
b) gcd(47,20)=(20,7)=(7,6)=(6,1)=1
c) gcd(43,35)=(35,8)=(8,3)=(3,2) =(2,1)=1

20) Determinare λ , $\mu \in \mathbb{Z}$ tali che25 λ + 32 μ = 1, per mezzo dell'Algoritmo di Euclide esteso, ed utilizzare il risultato ottenuto per risolvere l'equazione 25 x ≡ 4 mod 32

SOLUZIONE
Euclide esteso:
$r_k = a_k \cdot 32 + b_k \cdot 25$

con:
$r_k = r_{k-2} - r_{k-1}$
$a_k = a_{k-2} - a_{k-1}$
$b_k = b_{k-2} - b_{k-1}$

partendo da:
$32 = 1 \cdot 32 + 0 \cdot 25$
$25 = 0 \cdot 32 + 1 \cdot 25$

si ha (esecuzione dell'algoritmo di Euclide):

rk	ak	bk
32	1	0
25	0	1
7	1	-1
4	-3	4
3	4	-5
1	-7	9

da cui si ottiene che: λ=9 e μ=-7, ovvero: $9 \cdot 25 - 7 \cdot 32 = 1$
da cui:
$9 \cdot 25 = 1 - \mu \cdot 32$
ovvero:
$9 \cdot 25 = 1 \mod 32$
che posso sfruttare per risolvere l'equazione 25x=4 mod 32, infatti:
25x=4 mod 32
$x = 25^{-1} \cdot 4 \mod 32$
$x = 9 \cdot 4 \mod 32 = 4 \mod 32$

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.

SOLUZIONE
n=77, $\Phi(n)=60$
e=13

Con l'algoritmo di Euclide:

rk	ak	bk
60	1	0
13	0	1
8	1	-4
5	-1	5
3	2	-9
2	-3	14
1	5	-23

si ottiene:
$1 = 5 \cdot 60 - 23 \cdot 13$
quindi::
$(-23) \cdot 13 = \mod 60$
$d = e^{-1} = (-23) = 37$

$m = 2^{37} \mod 77 = 51$
infatti:
$51^{13} \mod 77 = 2 = c$