Corso di Network Security
a.a. 2012/2013

Soluzione dei quesiti sulla prima parte del corso

---

1) Si consideri un semplice cifrario a sostituzione monoalfabetico 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: SEGRETO

SOLUZIONE
Nel caso si consideri un alfabeto di 21 caratteri:
Cipher text: $c = E_k(m) = E_4(\text{"SEGRETO"}) = \text{"ZIMVIAS"}$

Nel caso si consideri invece un alfabeto di 26 caratteri:
Cipher text: c = "WIKVIXS"

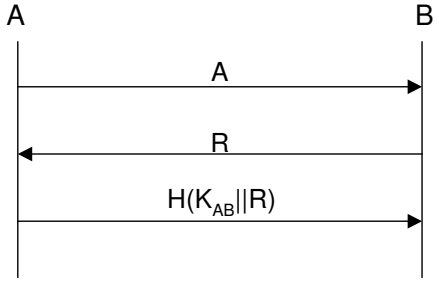
---

2) Sulla base di una funzione hash H() e di una chiave simmetrica K_{AB} condivisa tra due entità A e B, si chiede:

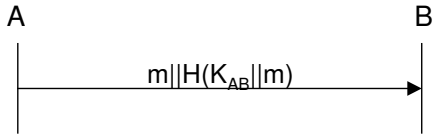
i) un possibile schema di autenticazione di A da parte di B (authenticator)
ii) di inviare un messaggio *m* da A a B garantendo l'autenticità/integrità dei dati inviati
iii) di costruire una possibile funzione di criptaggio (e la corrispondente funzione di decriptaggio) per inviare un messaggio *m* da A a B

SOLUZIONE

i) Possibile schema di autenticazione di A da parte di B (authenticator):



ii) A invia messaggio *m* garantendo autenticità/integrità:



iii) Costruzionie di una funzione di criptaggio:

$O_0 = IV$
$O_i = H(K_{AB} || O_{i-1})$
$o = O_1 || O_2 || O_3 || \ldots || O_n || \ldots$

$c = E_{KAB,IV}(m) = m \oplus o$

messaggio inviato:

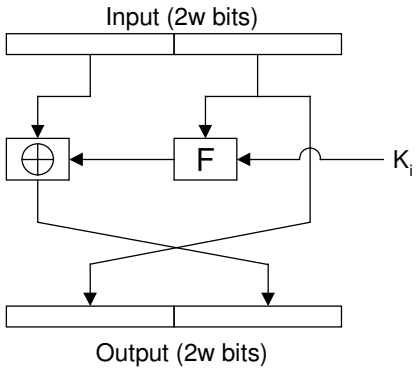
A→ B : x= IV||c

decriptaggio:
$m = D_{KAB,IV}(c) = c \oplus o$

---

3) Si indichi lo schema generale della struttura di un cifrario di Feistel. E' sufficiente indicare lo schema di un singolo round.

SOLUZIONE



---

4) 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:
$c_0=IV$
$c_i=Ek(m_i \oplus c_{i-1})$

---

5) Indicare la complessità di un attacco a forza bruta alla chiave segreta *K* di dimensione *n* bit utilizzata per criptare un messaggio *m* di dimensione *pq* bit tramite algoritmo di crittografia a blocchi $E_K()$ di dimensione *q* in modalità CBC, supponendo di conoscere: *m*, *c=E-CBC(K,m)*, e le funzioni $E_K()$ e $D_K()$ utilizzate. Si riporti la complessità in termini di numero di operazioni di criptaggio $E_K()$ e/o decriptaggio $D_K()$ dei singoli blocchi, in funzione di *n*, *p* e *q*.

SOLUZIONE
Partendo dal messaggio *m*, il numero massimo di chiavi che si devono provare (caso peggiore) per trovare *K* tale che *E-CBC(K,m)* $\equiv c$ è 2^n. Poiché ogni tentativo richiede l'esecuzione di *p* operazioni di criptaggio, la complessità di tale attacco è: **p 2^n**.
Stesso risultato si ottiene cercando *K* tale che *D-CBC(K,c)* $\equiv m$.

6) 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	*cinhertext*
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)

---

7) 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)

---

8) Si consideri un messaggio *m=M1||M2||M3||M4*, e si supponga di critparlo con un algoritmo di crittografia a blocchi $E_K()$ in modalità CBC (la dimensione dei blocchi di $E_K()$ è pari alla dimensione dei blocchi *Mi*), con *iv=IV0*, ottenendo il messaggio cifrato *c= C1||C2||C3||C4*.
Se un attaccante modifica il messaggio cifrato riarrangiando i blocchi che lo compongono componendo il messaggio cifrato c'= *C1||C3||C2||C4*, quale sarà il messaggio *m'=M'1||M'2||M'3||M'4* "erroneamente" decifrato a partire da *c'*? Indicare il valore dei blocchi *M'i* in funzione di *Mi* e *Ci*.

SOLUZIONE
Criptando in modalità CBC si ha:
$C_i = E_K(M_i \oplus C_{i-1})$
e:
$M_i = D_K(C_i) \oplus C_{i-1}$

e quindi anche:
$D_K(C_i) = M_i \oplus C_{i-1}$

Indicando con:
m' = M'1||M'2||M'3||M'4

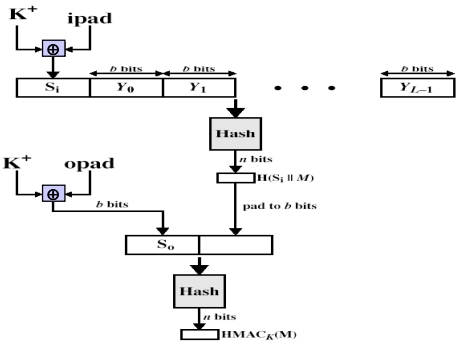
sapendo che
c'= *C1||C3||C2||C4*

si ricava che:
$M'1 = D_K(C'1) \oplus IV0 = D_K(C1) \oplus IV0 = M1$
$M'2 = D_K(C'2) \oplus C'1 = D_K(C3) \oplus C1 = (M3 \oplus C2) \oplus C1$
$M'3 = D_K(C'3) \oplus C'2 = D_K(C2) \oplus C3 = (M2 \oplus C1) \oplus C3$
$M'4 = D_K(C'4) \oplus C'3 = D_K(C4) \oplus C2 = (M4 \oplus C3) \oplus C2$

9) 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: ***N+3***

---

10) 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:
$o_i= Ek(o_{i-1})=AES(k,o_{i-1})$
$o_0=IV$

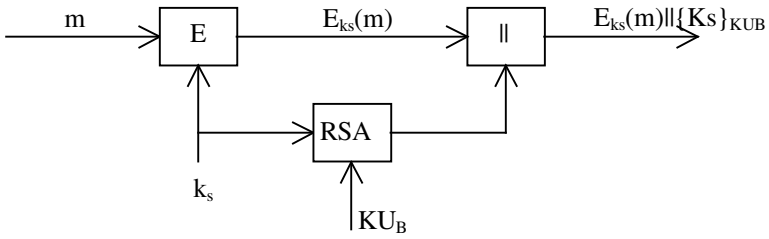
---

11) 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:**

SOLUZIONE

Invio:

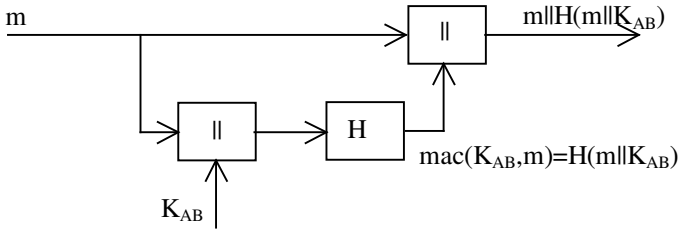


12) Si supponga di voler inviare in modo sicuro un messaggio *m* da A a B, garantendo SOLO l'autenticità/integrità dei dati inviati. Indicare schematicamente quali funzioni possono essere svolte in fase di invio/ricezione, supponendo che A e B condividano una chiave segreta K_{AB}, e che dispongano solo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

Invio: **Ricezione:**

SOLUZIONE

Invio:



13) Si supponga di voler inviare un messaggio *m* da A a B, garantendo sia la confidenzialità dei dati inviati che la loro autenticità/integrità. 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), e abbiano a disposizione i seguenti algoritmi di crittografia: RSA, AES, SHA1.

Invio: **Ricezione:**

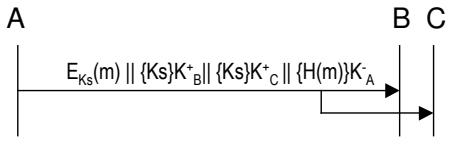
SOLUZIONE

dati inviati:
$x = AES_{Ks}(m) \,||\, RSA_{KUb}(Ks) \,||\, RSA_{KRa}(H(m))$

oppure:
$x = AES_{Ks}(m \,||\, RSA_{KRa}(H(m))) \,||\, RSA_{KUb}(Ks)$

14) Si supponga di voler inviare in modo sicuro un messaggio *m* da una sorgente A contemporaneamente a due destinazioni B e C, garantendo sia la confidenzialità dei dati inviati (tramite cifratura) che la loro integrità e autenticazione (tramite firma digitale). Per la cifratura del messaggio si utilizzi un algoritmo di crittografia simmetrica $E_k()$. Si supponga che A, B e C possiedano le loro rispettive chiavi RSA private, K^-_A, K^-_B e K^-_C , e che condividano tra loro solo le chiavi pubbliche K^+_A, K^+_B e K^+_C.
Indicare schematicamente quali funzioni sono svolte da A in fase di invio, e quale è il messaggio *x* effettivamente spedito da A a B e C.

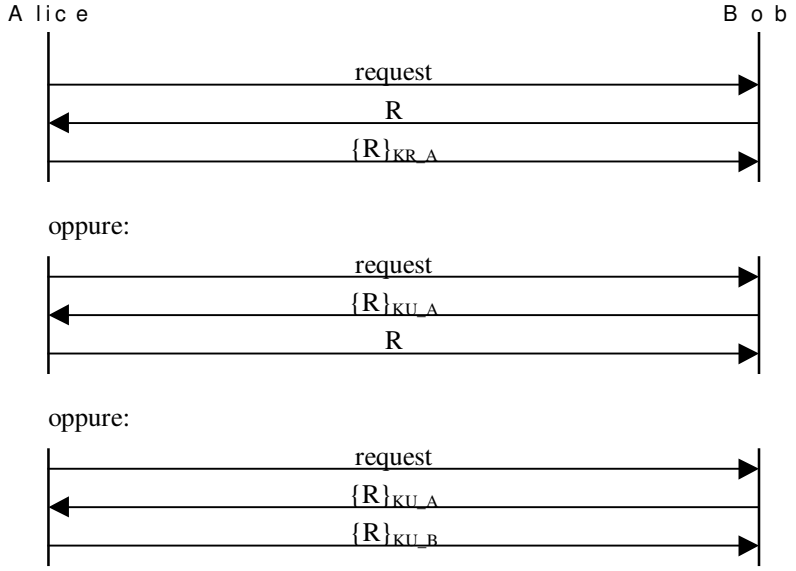
SOLUZIONE
Inivio:



Dati inviati: $x = E_{Ks}(m) \,||\, \{Ks\}K^+_B \,||\, \{Ks\}K^+_C \,||\, \{H(m)\}K^-_A$

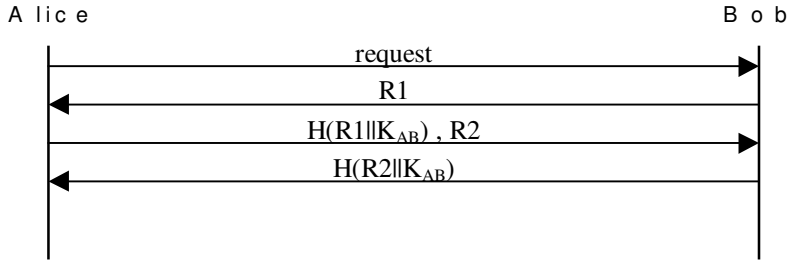
15) Indicare un possibile schema sicuro di autenticazione tra Alice (supplicant) e Bob (authenticator), nell'ipotesi che Alice e Bob condividano le rispettive chiavi RSA pubbliche KU_A e KU_B (si indichino con KR_A e KR_B le corrispondenti chiavi private).

SOLUZIONE



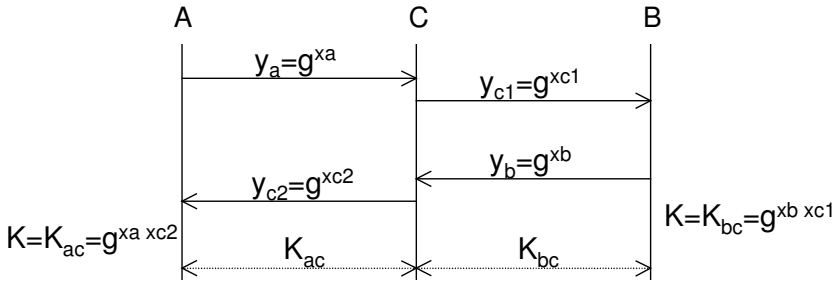
16) Indicare un possibile schema sicuro di mutua autenticazione tra due utenti Alice e Bob, basato sull'uso di una funzione hash H(·) e su un segreto condiviso K_{AB}.

SOLUZIONE



17) 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



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

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

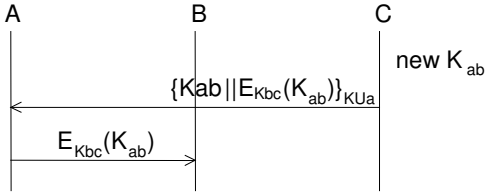
ii) C possieda la chiave pubblica di A, KU_A;

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 (ovvero una chiave segreta K_{AB}).

SOLUZIONE
Un possibile schema che permette ad A e B di ottenere una chiave condivisa K_{AB} è il seguente:



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

Osservazione:
Volendo proteggere lo scambio di chiave anche da attacchi di tipo replay e/o sostituzione si può ricorrere ad uno schema tipo Needham-Schroeder dove C agisce da *trusted-third party* (KDC) tra A e B, dove però viene usata tra A e C la chiave pubblica di A al posto di quella segreta simmetrica Kac:
A → C: IDa,IDb,Na
C → A: $\{Kab,IDb,Na,\{Kab,IDa\}_{Kbc}\}_{KUa}$
A → B: $\{Kab,IDa\}_{Kbc}$
B → A: $\{Nb\}_{Kab}$
A → B: $\{Nb-1\}_{Kab}$

---

19) Nell'ipotesi che A possieda i seguenti certificati digitali: $cert_{CA3}(A)$, $cert_{CA2}(CA3)$, $cert_{CA1}(CA2)$, e $cert_{CA1}(CA1)$ (dove è indicato con $cert_Y(X)$ 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:
$cert_{CA1}(CA1)$	$cert_{CA3}(A)$, $cert_{CA2}(CA3)$, $cert_{CA1}(CA2)$
$cert_{CA3}(A)$	nulla (nessun certificato, solo l'identità di A)
$cert_{CA1}(CA2)$	$cert_{CA3}(A)$, $cert_{CA2}(CA3)$
$cert_{CA1}(CA1)$, $cert_{CA3}(A)$	nulla (nessun certificato, solo l'identità di A)

20) Se A possiede $cert_B(A)$ e $cert_C(B)$ (dove si è indicato con $cert_Y(X)$ il certificato di X firmato da Y), mentre D possiede $cert_E(D)$, 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).

---

21) 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 $ed=1 \bmod 20$
e e d possono essere usate rispettivamente come chiave pubblica e privata per cifrare decifrare m; quidi:
$c=E(m)=2^7 \bmod 33=29$
si può verificare che:
$m=D(c)=29^3 \bmod 33=((29x29) \bmod 33) \bmod 33)=16x29 \bmod 33=2$

---

22) 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 $ya=g^{xa} \bmod p=10$
B invia ad A $ya=g^{xb} \bmod p=8$
dati ya e xb, B costruisce: $Kba=ya^{xb} \bmod p=10^3=100x10=1x10=10$
dati yb e xa, A costruisce $Kab= yb^{xa} \bmod p=8^5=(8^2)^2x8=2^2x8=4x8=10$
giustamente si ha Kab=Kba

---

23) 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

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

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:
$32=1\cdot32 + 0\cdot25$
$25=0\cdot32 + 1\cdot25$

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: $\lambda=9$ e $\mu=-7$, ovvero: $9\cdot25 - 7\cdot32 = 1$
da cui:
$9\cdot25 = 1 -\mu\cdot32$
ovvero:
$9\cdot25 = 1 \bmod 32$

che posso sfruttare per risolvere l'equazione $25x=4 \bmod 32$, infatti:
$25x=4 \bmod 32$
$x=25^{-1}\cdot4 \bmod 32$
$x =9\cdot4 \bmod 32=4 \bmod 32$

25) 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:
$1=5\cdot60-23\cdot13$
quindi::
$(-23)\cdot13 = \bmod 60$
$d=e^{-1}=(-23)=37$

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