

1. Definire formalmente il concetto di perfetta sicurezza.

SUPPONIAMO DI AVERE UN CIFRARIO SIMMETRICO, SE = {K, Enc, Dec} E SIANO K, M, C INSIEMI NON VUOTI, $\forall m_1, m_2 \in M$ e $\forall c \in C$

DEVE VALERE:

$$P[Enc(K, m_1) = c] = P[Enc(K, m_2) = c]$$

2. Sia SE = (KeyGen, Enc, Dec) un cifrario simmetrico e siano M, K, C gli insiemi dei messaggi, delle chiavi e dei crittostessi, rispettivamente.

Si considerino adesso i seguenti insiemi

$$M = \{1, 2, 3\} \quad K = \{1, 2, 3\}$$

Supponiamo di voler cifrare un solo messaggio $m \in M$, utilizzando una chiave (random) $k \in K$, come segue

$$c = (k \cdot m) \bmod 7$$

E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$n=1 \quad M=\{1, 2, 3\} \quad K=3$$

$$c=1 \quad c=3$$

$$c=2 \quad c=6$$

$$c=3 \quad c=2$$

$$n=2 \quad m_1=1 \quad m_2=2 \quad c=1$$

$$c=4 \quad P[Enc(K, m_1) = c] = \frac{1}{3}$$

$$c=6 \quad P[Enc(K, m_2) = c] = 0$$

QUINDI "SE" NON È SICURO IN SENSO PERFETTO

3. Supponendo di avere a disposizione le procedure *Espandi_Chiave*, *S*, *Shift_Rows* e *mix_cols* discusse a lezione (delle quali non è richiesta, in questa sede, la descrizione algoritmica) si descriva dettagliatamente il funzionamento di AES, fornendo, inoltre, lo pseudocodice dell'algoritmo.

AES_n(M) {
 $(K_0, \dots, K_{10}) \leftarrow \text{Espandi_Chiave}(K)$
 $S \leftarrow M \oplus K_0$
 for r = 1 to 10 do:
 $S \leftarrow S(S)$
 $S \leftarrow \text{Shift_rows}(S)$
 if ($r \leq 9$) then $\text{mix_cols}(S)$
 $S \leftarrow S \oplus K_r$
 return S
}}

Per la descrizione dell'algoritmo guardare la teoria.

4. Definire formalmente il concetto di funzione pseudocasuale sicura.

SIA $F: K \times \{0,1\}^L \rightarrow \{0,1\}^L$ DEFINISCONO UN AVVERSARIO CHE DEVE CAPIRE SE SI STA ESEGUEndo UNA FUNZIONE CASUALE O UNA PSEUDO CASUALE, UTILIZZANDO F IN ACCESSO BLACK-BOX (ORAColo).

$\text{Esp}^{pnf-1}(A) :$ $K \leftarrow R_K$
 $b \leftarrow A^{f_n}$
 Return b

$\text{Esp}^{pnf-0} :$ Esp^{pnf-0}
 $\delta \leftarrow \text{Func}(D, R)$
 $\delta_b \leftarrow A^\delta$
 return b

$$\text{Adv}_{F'}^{pnf}(A) = P_r[\text{Esp}^{pnf-1}(A) = 1] - P_r[\text{Esp}^{pnf-0}(A) = 1]$$

QUESTO VANTAGGIO DEVE ESSERE VICINO A ZERO PER AFFERMARE CHE LA PRF SIA COMPUTAZIONALMENTE INDISTINGUIBILE DA UNA FUNZIONE CASUALE. $\forall A$.

5. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ una funzione pseudocasuale sicura. Siano inoltre $\alpha, \beta \in \{0,1\}^\ell$ due stringhe di bit note. Vogliamo utilizzare F per costruire una funzione $G : \{0,1\}^k \times \{0,1\}^{2\ell} \rightarrow \{0,1\}^\ell$, nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

```

 $G_k(x)$ 
Sia  $x = x_L \parallel x_R$            //  $|x_L| = |x_R| = \ell$ 
 $y_1 \leftarrow F_k(x_L \oplus \alpha)$ 
 $y_2 \leftarrow F_k(x_R \oplus \beta)$ 
 $y \leftarrow y_1 \oplus y_2$ 
return  $y$ 

```

Dimostrare formalmente che G non è una funzione pseudo-casuale sicura.

$$\begin{aligned}
 x_L &= x_R = \{0\}^\ell \\
 y_1 &\leftarrow x_L \oplus \alpha \\
 y_2 &\leftarrow x_R \oplus \beta \\
 y &\leftarrow x_L \oplus y_1 \oplus x_R \oplus y_2 \\
 y &\leftarrow \alpha \oplus \beta
 \end{aligned}$$

```

A(F) {
     $x_\alpha = x_\beta = \{0\}^\ell$ 
     $y \leftarrow O_{\text{prf}}(x_L \parallel x_R)$ 
    if ( $y = \alpha \oplus \beta$ ) return 1
    else return 0
}

```

$$\begin{aligned}
 \Pr_n [\text{Esp}^{\text{prf}-1}(A) = 1] &= 1 \\
 \Pr_n [\text{Esp}^{\text{prf}-0}(A) = 1] &= \frac{1}{2^\ell}
 \end{aligned}
 \Rightarrow \text{Adv}_n(A) \gg 0$$

27 Aprile 2012

martedì 26 ottobre 2021 19:27

- Definire formalmente il concetto di perfetta sicurezza.

SIA SE = (KeyGen, Enc, Dec) UN CIFRARIO A BLOCCHI E SIANO $\mathcal{M}, \mathcal{K}, \mathcal{C}$ GLI INSIEMI DEI MESSAGGI, DELLE CHIAVI E DEI CRITTOTESTI, ALLORA:

$$\Pr[Enc(k, m_1) = c] = \Pr[Enc(k, m_2) = c]$$

- Sia SE = (KeyGen, Enc, Dec) un cifrario simmetrico e siano $\mathcal{M}, \mathcal{K}, \mathcal{C}$ gli insiemi dei messaggi, delle chiavi e dei crittostest, rispettivamente.

Si considerino adesso i seguenti insiemi

$$\mathcal{M} = \{1, 2, 3, 4, 5\} \quad \mathcal{K} = \{1, 2, 3, 4, 5\}$$

Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

$$C = (k \cdot m) \bmod 6$$

E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$m_1 = 1 \quad m_2 = 4$$

$$\Pr[Enc(k, 1) = 1] = \frac{1}{5}$$

$$\Pr[Enc(k, 4) = 1] = 0$$

NON È PERFETTAMENTE SICURA

$$c = 4 \cdot 1 \bmod 6 = 4$$

$$c = 4 \cdot 2 \bmod 6 = 2$$

$$c = 4 \cdot 3 \bmod 6 = 0$$

$$c = 4 \cdot 4 \bmod 6 = 4$$

$$c = 4 \cdot 5 \bmod 6 = 2$$

3. Supponendo di avere a disposizione le procedure *Espandi_Chiave*, *S*, *Shift_Rows* e *mix_cols* discusse a lezione (delle quali non è richiesta, in questa sede, la descrizione algoritmica) si descriva dettagliatamente il funzionamento di AES, fornendo, inoltre, lo pseudocodice dell'algoritmo.

$\text{AES}_k(M)$ {

$(K_0, \dots, K_{t_0}) \leftarrow \text{ESPANDI-CHIAVE}(k)$

$S = M \oplus K_0$

for $r \leftarrow 1$ to t_0 do:

$S \leftarrow S(S)$

$S \leftarrow \text{Shift_rows}(S)$

if ($r \leq j$) then:

$S \leftarrow \text{Mix_Cols}(S)$

$S = S \oplus K_r$

return S

Per la descrizione guardare dell'algoritmo guardare la teoria.

4. Definire formalmente il concetto di funzione pseudocasuale sicura.

SIA $F: K \times \{0,1\}^l \rightarrow \{0,1\}^l$ UNA
FAMIGLIA DI FUNZIONI CASUALI, ALLORA

UNA FUNZIONE SI DEFINISCE PSEUDO-CASUALE SE USA UN SISTEMA DI FUNZIONI (n, d) DI QUESTE FUNZIONI.

PER DIMOSTRARE CHE SI TRATTÀ DI UNA FUNZIONE PSEUDOCASUALE BISOGNA COSTRUIRE UN AVV. A CHE NON SIA IN GRADO DI DISTINGUERE QUANDO SI USA UNA FUNZIONE CASUALE DA QUANDO SI USA UNA PRF.

SI DEVE AVERE:

$$\text{Adv}(A) = \Pr_r [\text{Esp}^{\text{Prf}^{-1}}(A) = 1] - \Pr_r [\text{Esp}^{\text{Prf}^{-0}}(A) = 1] \approx 0$$

5. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ una funzione pseudocasuale sicura. Vogliamo utilizzare F per costruire una funzione $G : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$, nel seguente modo

```

 $G_k(x)$ 
 $y_1 \leftarrow F_k(x)$ 
 $y_2 \leftarrow F_k(\bar{x}) \quad \bar{x} \text{ indica la stringa complementare di } x$ 
 $y \leftarrow y_1 \oplus y_2$ 
return y

```

Dimostrare formalmente che G non è una funzione pseudo-casuale sicura.

$m_1 = 0 \dots 0$

$x = 0 \dots 0 \quad \bar{x} = 1 \dots 1 \quad y_1 \oplus y_2$

$m_2 = 1 \dots 1$

$x = 1 \dots 1 \quad \bar{x} = 0 \dots 0 \quad y_1 \oplus y_2$

$$A(G) := \{0\}^l$$

$$m_1 = \{1\}^l$$

$$y_1 = G_n(m_1)$$

$$y_2 = G_n(m_2)$$

if $y_1 \oplus y_2 = 0$ return 1

else return 0

$$\text{Adv}(A) = l - \frac{l}{2^l} \gg 0$$

1. In classe abbiamo definito il concetto di perfetta sicurezza nel seguente modo.

Sia $\text{SE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ un cifrario simmetrico e siano $\mathcal{M}, \mathcal{K}, \mathcal{C}$ gli insiemi dei messaggi, delle chiavi e dei crittotest, rispettivamente. Supponiamo di voler utilizzare SE per cifrare un solo messaggio. Diciamo che SE è *perfettamente sicuro* se $\forall M_1, M_2 \in \mathcal{M}$ e $\forall C \in \mathcal{C}$ si ha che

$$\Pr[\text{Enc}_k(M_1) = C] = \Pr[\text{Enc}_k(M_2) = C]$$

Si considerino adesso i seguenti insiemi

$$\mathcal{M} = \{0, 1, 2, 3, 4\} \quad \mathcal{K} = \{0, 1, 2, 3, 4\}$$

Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

$$C = (k + m) \bmod 5$$

E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$C_0 = 0, 1, 2, 3, 4$$

$$C_1 = 1, 2, 3, 4, 0$$

$$C_2 = 2, 3, 4, 0, 1$$

$$C_3 = 3, 4, 0, 1, 2$$

$$C_4 = 4, 0, 1, 2, 3$$

$$\Pr[\text{Enc}(k, m_1) = C] = \Pr[\text{Enc}(k, m_2) = C]$$

$\forall m \in \mathcal{M}, k \in \mathcal{K}, C \in \mathcal{C}$ vale

SENPRE

2. Definire formalmente il concetto di funzione pseudocasuale sicura.

SIA $F: \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$ UNA FAMIGLIA DI FUNZIONI
PESONALI DI QUESTA CONSIDERIAMO UN
SOTTOinsieme \mathcal{F} CHE PRENDANO IL NOME DI
PRF. UNA PRF È SICURA SE DATO UN
AVV. A CONTRA LA SICUREZZA PRF È CONSL,
DERANDA DUE RAND:

- RAND 0 \rightarrow SI UTILIZZA UNA FUNZIONE
CASUALE F
- RAND 1 \rightarrow SI UTILIZZA UNA FUNZIONE
PSEUDO-CASUALE

IL VANTAGGIO DI A CHE È IL
SEGUENTI:

$$\text{Adv}(A) = P_r[\text{Esp}^{\text{mf}-s}(A) = 1] - P_h[\text{Esp}^{\text{mf}-0}(A) = 1]$$

DEVE ESSERE UN VALORE PIUTTO VICINO
A ZERO.

3. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ una funzione pseudocasuale sicura (per semplicità si può assumere che F sia proprio una funzione casuale). Vogliamo utilizzare F per costruire una funzione pseudocasuale sicura $G : \{0,1\}^k \times \{0,1\}^{2\ell} \rightarrow \{0,1\}^{2L}$. Supponiamo di voler realizzare G nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

```

 $G_k(x)$ 
Sia  $x = L \parallel R$  //  $|L| = |R| = \ell$ 
 $y_L \leftarrow F_k(L)$ 
 $y_R \leftarrow F_k(R)$ 
 $y \leftarrow y_L \parallel y_R$ 
return y

```

E' G una buona (sicura) funzione pseudo-casuale? Giustificare formalmente la risposta fornita.

$A(G)$:

$$X = \{0\}^\ell$$

$X' \leftarrow X \parallel X$

$Y \leftarrow O_{P_A F}(X')$

if $Y_C = Y_R$ return 1
else return 0

$$\text{Adv}_V(A) = 1 - \frac{1}{2^L} > 0$$

4. In classe abbiamo descritto il modo ECB. Si tratta di un cifrario deterministico che utilizza, come primitiva di base, un cifrario a blocchi. In particolare l'algoritmo di cifratura è il seguente.

$\text{Enc}_k(M)$

if $(|M| \bmod n \neq 0) \vee (|M| = 0)$ return ⊥

Sia $M = M[1] \dots M[m]$ ($|M[i]| = n$)

for $i = 1$ to m do

$C[i] = E_k(M[i])$ // E_k è un cifrario a blocchi generico (ad es. AES).

$C \leftarrow C[1] \dots C[m]$

return C

Spiegare il funzionamento di tale algoritmo e fornire il corrispondente algoritmo di decifratura.

$\text{DEC}_k(M)$

if $(|C| \bmod n \neq 0) \vee (|M| = 0)$ return ⊥

Sia $C = C[1] \dots C[m]$ ($|C[i]| = n$)

for $i = 1$ to m do

$M[i] = \text{DEC}_k(C[i])$

$M \leftarrow M[1] \dots M[m]$

return M

5. Supponiamo che Alice voglia inviare il messaggio $M = M[1] \parallel \dots \parallel M[m]$, ($|M[i]| = n$) a Bob. Trattandosi di un messaggio privato, Alice decide di cifrarlo utilizzando ECB. Sia $C = C[1] \dots C[m]$ il crittostesto inviato da Alice. Supponiamo che uno dei blocchi di C , per esempio $C[2]$ (assumendo $m \geq 2$), venga trasmesso in modo incorretto. Quanti blocchi del messaggio originale M saranno influenzati da tale errore di trasmissione? Giustificare la risposta fornita.

I BLOCCHI DEL MESSAGGIO A RIGINCALÈ
NON SARANNO INFUENZATI A NENO DI
QUELLO CHE È STATO TRA SNESSO CON
ERRORE.

- Si considerino i seguenti insiemi

$$\mathcal{M} = \{000, 010, 111\} \quad \mathcal{K} = \{0, 1\}^3$$

(\mathcal{K} è dunque l'insieme di tutte le stringhe binarie di lunghezza 3).

Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

$$c = k \oplus m$$

E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$\Pr [\text{Enc}(k, m_1) = c] = \Pr [\text{Enc}(k, m_2) = c]$$

$\forall m_1, m_2 \in \mathcal{M}, m_1 \neq m_2, c \in \mathcal{C}, k \in \mathcal{K}$
con $\mathcal{K}, \mathcal{M}, \mathcal{C}$ INSIEMI FINITI

SE $m = 000$ ALLORA OTTENIAMO IN OUTPUT LA CHIAVE

SE $m = 111$ ALLORA OTTENIAMO IN OUTPUT LA CHIAVE
INVERTITA

SE $m = 010$ SI OTTIENE SEMPRE LA NUMERAZIONE
DA 0 A 7 IN BINARIO.

DA QUESTE AFFERMAZIONI POSSIAMO CONCLUDERE CHE
IL CIFRARIO È PERFETTAMENTE SICURO, PERCHÉ:

$\forall m_1, m_2 \in \mathcal{M}, \text{ con } m_1 \neq m_2 \text{ VALE CHE:}$

$$\Pr [\text{Enc}(k, m_1) = c] = \Pr [\text{Enc}(k, m_2) = c]$$

3. In classe, parlando del cifrario a blocchi AES,abbiamo discusso il campo di Galois $GF(2^8)$. Abbiamo visto che, in tale insieme, ogni byte può essere rappresentato come un polinomio di grado (al più) 7. Ricordando che $m(x) = x^8 + x^4 + x^3 + x + 1$ è il polinomio irriducibile discusso a lezione, si calcoli la somma ed il prodotto dei seguenti due byte:

$$x^7 + x^6 + x^5 + x^3 + x + 1$$

$$x^7 + x^5 + x^2 + x$$

$$\begin{array}{r} x^7 + x^6 + x^5 + x^3 + x + 1 \\ \hline x^7 + x^5 + x^2 + x \\ \hline x^6 + x^3 + x^2 + 1 \end{array} \quad \oplus$$

$$\begin{array}{r} x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^7 + \\ + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + \\ + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + \\ + x^8 + x^7 + x^6 + x^4 + x^2 + x = \end{array}$$

$$= x^{14} + x^{13} + x^{11} + x^9 + x^7 + x^4 + x^3 + x$$

$x^{14} + x^{13} + x^{11} + x^8 + x^7 + x^4 + x^3 + x$	$x^8 + x^4 + x^3 + x + 1$
$x^{14} + x^{10} + x^8 + x^7 + x^6$	$x^6 + x^5 + x^3 + x^2 + x + 1$
$\cancel{x^{13}} + x^{11} + x^{10} + x^8 + x^4 + x^3 + x$	
$\cancel{x^{11}} + x^9 + x^8 + x^6 + x^5$	
$\cancel{x^9} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^3 + x$	
$\cancel{x^9} + x^7 + x^6 + x^4 + x^5$	
$\cancel{x^6} + x^9 + x^8 + x^7 + x^6 + x^5 + x$	
$\cancel{x^6} + x^6 + x^5 + x^3 + x^2$	
$\cancel{x^5} + x^8 + x^7 + x^3 + x^2 + x$	
$\cancel{x^5} + x^5 + x^4 + x^2 + x$	
$\cancel{x^4} + \cancel{x^2} + x + 1$	

$$\frac{x^7 + x^5 + x + 1}{x^7 + x^5 + x + 1}$$

5. Sia $F : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ una funzione pseudocasuale sicura. Vogliamo utilizzare F per costruire una funzione pseudocasuale $G : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^{2L}$, nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

```

 $G_k(x)$ 
 $y_L \leftarrow F_k(x)$ 
 $y_R \leftarrow F_k(\bar{x})$  //  $\bar{x}$  denota la stringa complemento di  $x$ 
 $y \leftarrow y_L \parallel y_R$ 
return y

```

1

- BISOGNA TROVARE UN COMPORTAMENTO ANOMALO RISPETTO LA CHIAVE
- SPIEGARE LA STRATEGIA

Dimostrare formalmente che G non è una buona (sicura) funzione pseudocasuale.

$$\begin{array}{ll} m_1 = 0 \dots 0 & \rightsquigarrow y = y_L \parallel y_R \\ m_2 = 1 \dots 1 & \rightsquigarrow y' = y'_L \parallel y'_R \end{array} \quad \left. \begin{array}{l} y_L = y'_R \wedge y_R = y'_L \end{array} \right\}$$

DA QUESTA OSSERVAZIONE POSSIAMO COSTRUIRE L'AVV. A :

A(G) :

$$\begin{aligned} m_1 &\leftarrow \{0\}^\ell \\ m_2 &\leftarrow \{1\}^\ell \\ y_1 &\leftarrow G_K(m_1) \\ y_2 &\leftarrow G_K(m_2) \\ \text{if } (y_1^1 = y_2^2 \wedge y_1^2 = y_2^1) &\text{return 1} \\ \text{else return 0} \end{aligned}$$

$$\Pr[\text{Esp}^{\text{PnF-L}}(A) = 1] = 1$$

$$\Pr[\text{Esp}^{\text{PnF-O}}(A) = 1] = \frac{1}{2^{2L}}$$

$$\text{Adv}(A) = 1 - \frac{1}{2^{2L}} \gg 0 \rightarrow \text{NON È UNA BUONA PRF}$$

$A(G)$:

$$x \leftarrow \{0, 1\}^L$$

$$y \leftarrow O_{\text{PRF}}(x)$$

$$z \leftarrow O_{\text{PRF}}(\bar{x}) ; \quad z = z_L \parallel z_R$$

if ($y_L == z_R$) \wedge ($y_R == z_L$) return 1
else return 0

$$\Pr[\text{Esp}^{\text{PnF-L}}(A) = 1] = 1$$

$$\Pr[\text{Esp}^{\text{PnF-O}}(A) = 1] = \frac{1}{2^{2L}}$$

1. Definire formalmente il concetto di perfetta sicurezza.

SIANO:

- K L'INSIEME DELLE CHIAVI;
- M L'INSIEME DEI MESSAGGI;
- C L'INSIEME DEI CRIPTOTESTI.

TUTTI E TRE INSIEMI FINITI. SI DEFINISCE PERFETTA SICUREZZA, QUANDO $\forall m_1, m_2 \in M \wedge m_1 \neq m_2 \wedge \forall c \in C$ SI HA:

$$\Pr[Enc(k, m_1) = c] = \Pr[Enc(k, m_2) = c]$$

2. In classe abbiamo discusso il cifrario One Time Pad, che qui richiamiamo. Sia M lo spazio dei messaggi, K lo spazio delle chiavi e C lo spazio dei crittotestni, con $M = K = C = \{0, 1\}^\ell$ (ℓ parametro fissato). L'algoritmo di generazione delle chiavi KeyGen, su input ℓ , restituisce una chiave random in K . L'algoritmo di cifratura, Enc, prende in input una chiave $k \in K$ ed un messaggio $m \in M$ e restituisce un crittoresto $c = k \oplus m$. Infine l'algoritmo Dec prende in input una chiave $k \in K$ ed un crittoresto $c \in C$ e restituisce un messaggio $m = c \oplus k$.

Supponiamo di voler utilizzare One Time Pad per cifrare un solo messaggio. Si dimostri che, se utilizzato in questo modo, One Time Pad offre perfetta sicurezza.

PRESI $m_1, m \in M \wedge m_1 \neq m_2 \wedge K$ ESTRATTA CASUALMENTE DA K SI HA CHE:

$$\Pr[Enc(k, m_1) = c] = \frac{1}{2^\ell}$$

QUESTO PERCHÉ ESISTE UNA SOLA CHIAVE CHE PRESO IL MESSAGGIO m_1 PERMETTE DI GENERARE c . LA STESSA COSA VALE PER m_2 , INFATTI:

$$\Pr[Enc(k, m_2) = c] = \frac{1}{2^\ell}$$

$$\Pr[\text{Enc}(k, m_2) = c] = \frac{1}{2^e}$$

DA QUI SEGUE LA DEFINIZIONE DI PERFETTA SICUREZZA:

$$\Pr[\text{Enc}(k, m_1) = c] = \Pr[\text{Enc}(k, m_2) = c]$$

$$\forall m_1, m_2 \in M \quad \& \quad m_1 \neq m_2 \quad \& \quad c \in C$$

5. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ una funzione pseudocasuale sicura. Vogliamo utilizzare F per costruire una funzione pseudocasuale $G : \{0,1\}^k \times \{0,1\}^{2\ell} \rightarrow \{0,1\}^{2\ell}$, nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

```

 $G_k(x)$ 
Sia  $x = x_L \parallel x_R$  //  $|x_L| = |x_R| = \ell$ 
 $y_L \leftarrow x_L \oplus F_k(x_R)$ 
 $y_R \leftarrow x_R \oplus F_k(x_L)$ 
 $y \leftarrow y_L \parallel y_R$ 
return y

```

Dimostrare formalmente che G non è una funzione pseudo-casuale sicura.

$A(G) :$

```

 $x_L = \{0\}^\ell = x_R$ 
 $y \leftarrow O_{\text{PRF}}(x_L \parallel x_R)$ 
if ( $y_L = y_R$ ) return 1
else return 0

```

INFATTI SE :

$$x_L = \{0\}^\ell \text{ SI HA CHE: } y_L = x_L \oplus F_k(x_R)$$

$$x_R = \{0\}^\ell \text{ QUINDI } y_R = y_L \text{ SE QUESTO È VERO}$$

ALLORA L'AVVERSARIO È CERTO DI UTLIZZARE

LA PRF.

VALE PER QUALUNQUE k

1

$$\text{Adv}(A) = \Pr_{\text{rv}} [E_{Sp}^{\text{perf-1}}(A)] - \Pr_{\text{rv}} [E_{Sp}^{\text{perf-0}}(A)] =$$
$$= 1 - \frac{1}{2} >> 0$$

- Definire formalmente il concetto di perfetta sicurezza.

SIANO :

- M , l'insieme dei messaggi;
- C , l'insieme dei crittostesti;
- K , l'insieme delle chiavi.

TUTTI E TRE GLI INSIEMI SONO FINITI, ACCORDA
SE $\forall m_1, m_2 \in M \wedge m_1 \neq m_2 \wedge \exists c \in C$ con
 $k \in K$:

$$\Pr[\text{Enc}(k, m_1) = c] = \Pr[\text{Enc}(k, m_2) = c]$$

IN QUESTO CASO SI PARLA DI PERFETTA SICUREZZA.

- Supponiamo che due utenti, Alice e Bob, vogliano usare One Time Pad per proteggere le loro comunicazioni. Alice, tuttavia, non è del tutto convinta della sicurezza offerta dal cifrario. In particolare, la preoccupa il fatto che se la chiave utilizzata dovesse essere la stringa nulla, il crittostesto prodotto sarebbe uguale al messaggio di partenza. Quindi Alice propone a Bob di usare la seguente variante, che potremmo chiamare OTP+. Lo spazio dei messaggi M e lo spazio dei crittostesti C sono dati da $\{0, 1\}^\ell$ (ℓ parametro fissato), mentre lo spazio delle chiavi $K = \{0, 1\}^\ell - \{0^\ell\}$. Per il resto il cifrario rimane identico a One Time Pad: l'algoritmo di cifratura, Enc , prende in input una chiave $k \in K$ ed un messaggio $m \in M$ e restituisce un crittostesto $c = k \oplus m$. Infine l'algoritmo Dec prende in input una chiave $k \in K$ ed un crittostesto $c \in C$ e restituisce un messaggio $m = c \oplus k$.

Supponiamo di voler utilizzare OTP+ per cifrare un solo messaggio. È tale metodo perfettamente sicuro? Giustificare la risposta fornita.

SUPPONIAMO DI UTILIZZARE $m_1 = \{0\}^\ell$ e $c = \{0\}^\ell$
ACCORA:

$$\Pr[\text{Enc}(k, m_1) = c] = \Pr[k \oplus \{0\}^\ell = \{0\}^\ell] = 0$$

QUESTO PERCHÉ L'UNICO modo PER OTTENERE c

QUESTO PERCHÉ L'UNICO MODO PER OTTENERE C
 È AVERE $\kappa = \{0\}^\ell$ CHE PERÒ È STATA ELIMINATA,
 MENTRE $\kappa \in \mathbb{M}$ SI HA CHE:

$$\Pr[\text{Enc}(x, \kappa) = c] = \frac{1}{|\mathbb{K}|}$$

5. Sia $F : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ una permutazione pseudocasuale sicura contro attacchi di tipo CPA. Vogliamo utilizzare F per costruire una **funzione** pseudocasuale $G : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^{2\ell}$, nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

$$G_k(x) = (F_k(x) \oplus x) \parallel F_k(x)$$

Dimostrare formalmente che G non è una funzione pseudo-casuale sicura.

$$\begin{aligned} A(G) : \\ x &\in \{0, 1\}^\ell \\ y &\leftarrow O_{PRP}(x) \end{aligned}$$

$$y' \leftarrow (F_k(x) \oplus x)$$

$$y'' \leftarrow F_k(x)$$

if ($y' \oplus y'' = x$) return 1
 else return 0

$$\Pr[\text{E}_{\text{SP}}^{\text{PRP-1}}(A) = 1] = 1$$

$$\Pr[\text{E}_{\text{SP}}^{\text{PRP-0}}(A) = 1] = \frac{1}{2^\ell}$$

$$\text{Adv}(A) = 1 - \frac{1}{2^\ell} \gg 0$$

QUINDI NON È UNA PRP.

12 Novembre 2007

lunedì 8 novembre 2021 17:15

1. In classe abbiamo definito il concetto di perfetta sicurezza nel seguente modo.

Sia $\text{SE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ un cifrario simmetrico e siano $\mathcal{M}, \mathcal{K}, \mathcal{C}$ gli insiemi dei messaggi, delle chiavi e dei crittostesti, rispettivamente. Supponiamo di voler utilizzare SE per cifrare un solo messaggio. Diciamo che SE è *perfettamente sicuro* se $\forall M_1, M_2 \in \mathcal{M}$ e $\forall C \in \mathcal{C}$ si ha che

$$\Pr[\text{Enc}_k(M_1) = C] = \Pr[\text{Enc}_k(M_2) = C]$$

Si considerino adesso i seguenti insiemi

$$\mathcal{M} = \{0, 1, 2, 3, 4, 5\} \quad \mathcal{K} = \{0, 1, 2, 3, 4, 5\}$$

Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

$$C = k + m$$

E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$m_1 = 0 \quad m_2 = 5 \quad C = 0$$

$$\Pr_n [\text{Enc}(k, 0) = 0] = \frac{1}{|\mathcal{K}|}$$

$$\begin{aligned} \Pr_n [\text{Enc}(k, 5) = 0] &= \Pr_n [0 = k + 5] = \\ &= \Pr_n [k = -5] = 0 \end{aligned}$$

4. Si consideri la seguente funzione $G : \{0, 1\}^k \times \{0, 1\}^k \rightarrow \{0, 1\}^k$. Supponiamo di voler realizzare G nel seguente modo:

$$G_k(x) = x \oplus k$$

E' G una buona (sicura) funzione pseudo-casuale? Giustificare formalmente la risposta fornita.

$$\text{Adv}^{\text{Pf}}(A) = \left| \Pr_n [\text{Exp}^{\text{Pf}-L}(A) = 1] - \Pr_n [\text{Exp}^{\text{Pf}-O}(A) = 1] \right|$$

$$m_1 = \{0\}^k$$

$A(G)$:

$$m_1 \leftarrow \{0\}^k$$

$$c_1 \leftarrow O_{\text{PRF}}^G(m_1)$$

$$c_2 \leftarrow O_{\text{PRF}}^G(c_1)$$

if ($c_2 = m_1$) return 1

$$c_1 = O_{\text{Pf}}(m_1) = m_1 \oplus k$$

$$\begin{aligned} c_2 &= O_{\text{Pf}}(c_1) = m_1 \oplus k \oplus k = \\ &= m_1 \end{aligned}$$

$C_2 \leftarrow \text{Uprf}(C_1)$ $C_2 = \text{Uprf}(C_1) = m_1 \oplus n \oplus n -$
if ($C_2 = m_1$) return 1 $= m_1$
else return 0

$$\Pr[ESP^{Pnf-1}(A) = 1] = 1$$

$$\Pr[ESP^{Pnf-0}(A) = 1] = \frac{1}{2^n}$$

2. Sia $\text{SE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ un cifrario simmetrico e siano $\mathcal{M}, \mathcal{K}, \mathcal{C}$ gli insiemi dei messaggi, delle chiavi e dei crittostessi, rispettivamente.

Si considerino adesso i seguenti insiemi

$$\mathcal{M} = \{1, 2, 3\} \quad \mathcal{K} = \{0, 1, 2, 3, 4, 5, 6\}$$

Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

$$C = ((k + 1) + m) \bmod 7$$

E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$K = 0$$

$$m = \underline{1}, 2, 3$$

$$C = \textcircled{0}, \textcircled{3}, \textcircled{4}$$

$$K = 1$$

$$C = \textcircled{3}, \textcircled{4}, \textcircled{5}$$

$$K = 2$$

$$C = \textcircled{4}, \textcircled{5}, \textcircled{6}$$

$$K = 3$$

$$C = \textcircled{5}, \textcircled{6}, \textcircled{0}$$

$$K = 4$$

$$C = \textcircled{6}, \textcircled{0}, \textcircled{1}$$

$$K = 5$$

$$C = \textcircled{0}, \textcircled{1}, \textcircled{2}$$

$$K = 6$$

$$\begin{aligned} \text{Enc}_K(m) &= (K+1)+m \bmod 7 \\ &= C \end{aligned}$$

$$K = (C - 1 - m) \bmod 7$$

$$c = \underline{1}, \underline{2}, \underline{3}$$

Possibile dimostrazione con il teorema
di Shannon 2 (da rivedere!)

$$\Pr [E_{nc}(n, \underline{m_1}) = \underline{c}] = \\ = \Pr [E_{nc}(n, \underline{m_2}) = \underline{c}]$$

$$k + 1 + m \bmod 7 = c$$

$$1 + m \bmod 7 = c - k$$

$$1 + m - c \bmod 7 = k$$

$$k + m \bmod 7 = c$$

2. Sia $\text{SE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ un cifrario simmetrico e siano $\mathcal{M}, \mathcal{K}, \mathcal{C}$ gli insiemi dei messaggi, delle chiavi e dei crittostesti, rispettivamente.

Si considerino adesso i seguenti insiemi

$$\mathcal{M} = \{1, 2, 3\} \quad \mathcal{K} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

$$C = (5m + k) \bmod 11$$

E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$\mathcal{C} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$C = (5m + k) \bmod 11$$

$$k = (C - 5m) \bmod 11$$

$$\Pr [\text{Enc}_k(m_1) = C] = \Pr [\text{Enc}_k(m_2) = C]$$

$$\Pr [k = (C - 5m_1) \bmod 11] = \Pr [k = (C - 5m_2) \bmod 11]$$

5. Sia $F : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ una permutazione pseudocasuale (sicura). Vogliamo utilizzare F per costruire una funzione $G : \{0, 1\}^k \times \{0, 1\}^{\ell+1} \rightarrow \{0, 1\}^\ell$, nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

$$G_k(x)$$

Sia $x = x_1 \dots x_{\ell+1}$ // x_i indica l'i-esimo bit di x

Poniamo $z = x_1 \dots x_\ell$

$y \leftarrow F_k(\bar{z})$ // \bar{z} indica la stringa complementare di z
return y

Dimostrare formalmente che G non è una funzione pseudo-casuale sicura.

Consideriamo due messaggi y e z così:

$$X = \{0, 1\}^e$$

$$Y = \underline{X} \amalg 0$$

$$Z = \underline{X} \amalg 1$$

$$a = G_n(Y) = F_n(\bar{X})$$

$$b = G_n(Z) = F_n(\bar{X})$$

SE $a = b$ return 1

ALTRIMENTI return 0

Formalizzazione:

$A(G)$:

$$X \leftarrow \{0, 1\}^e$$

$$Y \leftarrow X \amalg 0$$

$$Z \leftarrow X \amalg 1$$

$$a \leftarrow O_{\text{prp}}(Y)$$

$$b \leftarrow O_{\text{prp}}(Z)$$

if $a == b$ return 1

else return 0

$$\Pr [\text{Esp}^{\text{RP}} - \mathcal{L}(A) = 1] = 1$$

$$\Pr [\text{Esp}^{\text{RP}} - \mathcal{O}(A) = 0] = \frac{1}{2}$$

$$\text{Adv}_v(A) = 1 - \frac{1}{2} >> 0$$

3. In classe, parlando del cifrario a blocchi AES, abbiamo discusso il campo di Galois GF(2⁸). Abbiamo visto che, in tale insieme, ogni byte può essere rappresentato come un polinomio di grado (al più) 7. Ricordando che $m(x) = x^8 + x^4 + x^3 + x + 1$ è il polinomio irriducibile discusso a lezione, si calcoli la somma ed il prodotto dei seguenti due byte:

$$x^7 + x^6 + x^2 + 1 \quad x^6 + x^2 + x$$

$$\begin{aligned} & x^{13} + x^3 + \cancel{x^8} + x^{12} + \cancel{x^8} + x^7 + x^8 + x^4 + x^3 + \\ & + x^6 + x^2 + x = \end{aligned}$$

$$\begin{aligned} & = x^{13} + x^{12} + x^3 + x^8 + x^7 + x^6 + x^4 + x^3 + \\ & + x^2 + x = \end{aligned}$$

$$x^{13} + x^{12} + x^3 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x \quad | x^8 + x^4 + x^3 + x + 1$$

$$x^{13} + x^3 + x^8 + x^6 + x^5 \quad | x^5 + x^4 + 1$$

$$x^{12} + x^7 + x^5 + x^4 + x^3 + x^2 + x$$

$$\begin{array}{r} x^{12} + x^8 + x^7 + x^5 + x^4 \\ \hline x^8 + x^3 + x^2 + x \end{array}$$

$$x^8 + x^4 + x^3 + x + 1$$

$$\hline x^4 + x^2 + 1$$

$$\overline{x^8 + x^3 + x^2 + x}$$

$$\overline{x^8 + x^4 + x^3 + x + 1}$$

$$\overline{x^4 + x^2 + 1}$$

2. Sia $\text{SE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ un cifrario simmetrico e siano $\mathcal{M}, \mathcal{K}, \mathcal{C}$ gli insiemi dei messaggi, delle chiavi e dei crittotestimi, rispettivamente.

Si considerino adesso i seguenti insiemi

$$\mathcal{M} = \{0, 1\}^\ell, \quad \mathcal{K} = \{0, 1\}^{2\ell}$$

Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

$$C = (m || 0^\ell) \oplus k$$

(il simbolo $||$ indica l'operazione di concatenazione) E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$C \in \{0, 1\}^{2\ell}$$

considero $m_1 \in \mathcal{M}$:

$$\Pr [\text{Enc}_k(m_1) = C] =$$

$$\Pr [C = (m_1 || 0^\ell) \oplus k]$$

Possiamo scrivere $k = k' || k''$ con
 $k', k'' \in \{0, 1\}^\ell$

A questo punto:

$$\begin{aligned} & \Pr [C = (m_1 || 0^\ell) \oplus (k' || k'')] = \\ &= \Pr [C = (m_1 \oplus k') || (0^\ell \oplus k'')] = \\ &= \Pr [C' || C'' = (m_1 \oplus k') || (0^\ell \oplus k'')] \end{aligned}$$

$C' = m_1 \oplus k' \rightarrow \text{ONE-TIME PAD}$

$$C'' = 0^\ell \oplus k''$$

$$\Pr[Enc_k(m) = c] = \frac{1}{2^e} \quad \forall m \in M, \forall c \in C$$

$$C = \{0,1\}^{2^e}$$

$$C = (m || 0^e) \oplus K$$

$$K = C \oplus (m || 0^e)$$

3. In classe, parlando del cifrario a blocchi AES, abbiamo discusso il campo di Galois GF(2⁸). Abbiamo visto che, in tale insieme, ogni byte può essere rappresentato come un polinomio di grado (al più) 7. Ricordando che $m(x) = x^8 + x^4 + x^3 + x + 1$ è il polinomio irriducibile discusso a lezione, si calcoli la somma ed il prodotto dei seguenti due byte:

$$x^7 + x^5 + x^3 \quad x^7 + x^6 + x^2 + x + 1$$

$$\begin{aligned} & x^{14} + x^{13} + \cancel{x^8} + x^8 + \cancel{x^7} + \\ & + \cancel{x^{12}} + x^{11} + \cancel{x^7} + x^6 + \cancel{x^5} + \\ & + \cancel{x^{10}} + \cancel{x^5} + \cancel{x^5} + x^4 + x^3 = \end{aligned}$$

$$= x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^4 + x^3$$

$x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^4 + x^3$	$x^8 + x^4 + x^3 + x + 1$
$x^{14} + x^{10} + x^9 + x^7 + x^6$	$x^6 + x^5 + x^4 + x^3 + 1$
$x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^4 + x^3$	
$x^{13} + x^9 + x^8 + x^6 + x^5$	
$x^{12} + x^{11} + x^7 + x^6 + x^5 + x^4 + x^3$	

$$\begin{array}{r}
 x^{12} + x^{11} + x^7 + x^6 + x^5 + x^4 + x^3 \\
 \hline
 x^{12} + x^8 + x^7 + x^5 + x^4 \\
 \hline
 x^{11} + x^8 + x^6 + x^4 + x^3 \\
 \hline
 x^8 + x^7 + x^4 \\
 \hline
 x^8 + x^4 + x^3 + x + 1 \\
 \hline
 x^7 + x^3 + x + 1
 \end{array}$$

5. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^{2\ell}$ una funzione pseudocasuale sicura. Vogliamo utilizzare F per costruire una funzione $G : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^{3\ell}$, nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

```

 $G_k(x)$ 
 $z \leftarrow F_k(x)$ 
Sia  $z = z_1 \parallel z_2$  //  $|z_1| = |z_2| = \ell$ 
 $y \leftarrow z_1 \parallel z_2 \parallel (z_1 \oplus z_2)$ 
return y

```

Dimostrare formalmente che G non è una funzione pseudo-casuale sicura.

$$\begin{array}{ccc}
 z_1 \parallel z_2 \parallel (z_1 \oplus z_2) \\
 || \quad || \quad || \\
 Y^1 \quad Y^2 \quad Y^{14}
 \end{array}$$

$$Y^1 \oplus Y^2 \oplus Y^{14} =$$

$$= z_1 \oplus z_2 \oplus (z_1 \oplus z_2) = 0^\ell$$

FORNIRELLAZIA AL CAVVERSARIO:

$A(G)$:

$$x \in \{0,1\}^2$$

$$\gamma \leftarrow O_{\text{PRF}}(x); \gamma = \gamma' \parallel \gamma'' \parallel \gamma'''$$

if ($\gamma' \oplus \gamma'' \oplus \gamma''' = \text{o}^e$) return 1
else return 0

$$\Pr[E_{\text{SP}}^{\text{PRF-1}}(A) = 1] = 1$$

$$\Pr[E_{\text{SP}}^{\text{PRF-0}}(A) = 1] = \frac{1}{2^e}$$

$$\text{Adv}(A) = 1 - \frac{1}{2^e} \gg 0$$

2. Sia $\text{SE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ un cifrario simmetrico e siano $\mathcal{M}, \mathcal{K}, \mathcal{C}$ gli insiemi dei messaggi, delle chiavi e dei crittotest, rispettivamente.

Si considerino adesso i seguenti insiemi

$$\mathcal{M} = \{0, 1, 2, 3\} \quad \mathcal{K} = \{0, 1, 2, 3, 4\}$$

Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

$$C = (2m + k) \bmod 7$$

E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$C \in \{0, 1, 2, 3, 4, 5, 6\}$$

Consideriamo un messaggio m_1 :

$$\Pr [E_{n c_k}(m_1) = c] = \\ \Pr [(2m_1 + k) \bmod 7 = c]$$

$$(c - 2m_1) \bmod 7 = k$$

$$\text{Se } c - 2m_1 > 5 \Rightarrow \exists k \in \mathbb{K}$$

$$c = 6 \quad m_1 = 0$$

$$6 > 5$$

Quindi:

$$\text{Se } m_1 = 0, \quad c = 6$$

$$\Pr [E_{n c_k}(0) = 6] = 0$$

SE $m_2 = 3$

$$P_n[E_{n \times k}(3) = 6] = \frac{1}{|T_k|} = \frac{1}{5}$$

QUINDI NON È SICURA IN SENSO
PERFETTO

3. In classe, parlando del cifrario a blocchi AES, abbiamo discusso il campo di Galois $GF(2^8)$. Abbiamo visto che, in tale insieme, ogni byte può essere rappresentato come un polinomio di grado (al più) 7. Ricordando che $m(x) = x^8 + x^4 + x^3 + x + 1$ è il polinomio irriducibile discusso a lezione, si calcoli la somma ed il prodotto dei seguenti due byte:

$$x^7 + x^6 + x^3 + x + 1 \quad x^6 + x^5 + x^2 + x$$

$$\begin{aligned} & x^{13} + x^{12} + \cancel{x^8} + \cancel{x^8} + \\ & + \cancel{x^{12}} + x^{11} + x^8 + \cancel{x^7} + \\ & + \cancel{x^3} + \cancel{x^8} + \cancel{x^5} + x^4 + \\ & + \cancel{x^7} + \cancel{x^6} + x^3 + \cancel{x^2} + \\ & + \cancel{x^6} + \cancel{x^5} + \cancel{x^2} + x = \end{aligned}$$

$$x^{13} + x^{11} + x^8 + x^4 + x^3 + x$$

$$x^8 + x^4 + x^3 + x + 1$$

$$\begin{array}{r} x^{13} + x^3 + x^8 + x^6 + x^5 \\ \hline x^{11} + x^9 + x^6 + x^5 + x^4 + x^3 + x \end{array}$$

$$x^5 + x^3 + x$$

$$\begin{array}{r} x^{11} + x^7 + x^6 + x^4 + x^3 \\ x^3 + x^7 + x^5 + x \\ x^3 + x^5 + x^4 + x^2 \\ \hline x^7 + x^4 + x^2 + x \end{array}$$

5. Sia $F : \{0,1\}^k \times \{0,1\}^{\ell+1} \rightarrow \{0,1\}^L$ una funzione pseudocasuale (sicura). Vogliamo utilizzare F per costruire una funzione $G : \{0,1\}^k \times \{0,1\}^{3\ell} \rightarrow \{0,1\}^L$, nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

```

 $G_k(x)$ 
Sia  $x = x_1 \parallel x_2 \parallel x_3$  //  $|x_1| = |x_2| = |x_3| = \ell$ 
 $y \leftarrow F_k(x_1 \oplus x_2 \parallel 0) \oplus F_k(x_2 \oplus x_3 \parallel 1)$ 
return y

```

Dimostrare formalmente che G non è una funzione pseudo-casuale.

$$x = x_1 \parallel x_2 \parallel x_3 ; x \in \{0,1\}^{3\ell}$$

$$F_k(x_1 \oplus x_2 \parallel 0) \oplus F_k(x_2 \oplus x_3 \parallel 1)$$

$$x_1 = 1^\ell$$

$$x_2 = 0^\ell$$

$$x_3 = 1^\ell$$

$$x_1 \oplus x_2 \parallel 0$$

$$x_2 \oplus x_3 \parallel 1$$

$$F_k(0 \parallel 1^\ell)$$

$$F_k(0 \parallel 1^\ell)$$



A(G):

$$x_1 \leftarrow \{1^\ell\}$$

$\vdash \quad \wedge \quad \sim$

$$x_2 \leftarrow \{0^e\}$$

$$x_3 \leftarrow \{1^e\}$$

$$y \leftarrow \text{Oper}(x_1 || x_2 || x_3)$$

if $y = 0$ return 1
else return 0

$$\Pr[\text{Esp}^{\text{prf}-1}(A) = 1] = 1$$

$$\Pr[\text{Esp}^{\text{prf}-0}(A) = 1] = \frac{1}{2^L}$$

2. Sia $\text{SE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ un cifrario simmetrico e siano $\mathcal{M}, \mathcal{K}, \mathcal{C}$ gli insiemi dei messaggi, delle chiavi e dei crittostesti, rispettivamente.

Si considerino adesso i seguenti insiemi

$$\mathcal{M} = \{1, 2, 3, 4, 5\} \quad \mathcal{K} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

$$C = (3m + k) \bmod 11$$

E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

$$\mathcal{C} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

CONSIDERIAMO $m_1 \in \mathcal{M}$

$$\Pr [E_{\text{Enc}_k}(m_1) = C] =$$

$$\Pr [(3m_1 + k) \bmod 11 = C] \Rightarrow$$

$$\Rightarrow (C - 3m_1) \bmod 11 = k$$

ESSENDO CHE $C = k$ ALLORA
TROVEREMO SEMPRE $\forall c \in \mathcal{C}$ e $\forall m \in \mathcal{M}$
UN'UNICA CHIAVE $k \in \mathcal{K}$ TALE CHE:

$$C = (3m + k) \bmod 11$$

$m \setminus k$	1	2	3	4	5	6	7	8	9	10
1	4	5	6	7	8	9	0	1	2	3
2	7	8	9	0	1	2	3	4	5	6
3	0	1	2	3	4	5	6	7	8	9
4	2	3	4	5	6	7	8	9	0	1
5	5	6	7	8	9	0	1	2	3	4

4	2	3	4	5	6	7	8	9	0	1
5	5	6	7	8	3	0	1	2	3	4

ABBIANO DIMOSTRATO CHE

$$\Pr[\text{Enc}_K(m_1) = c] = \Pr[\text{Enc}_K(m_2) = c]$$

$$\forall m_1, m_2 \in M \wedge \forall c \in C$$

3. In classe, parlando del cifrario a blocchi AES, abbiamo discusso il campo di Galois $GF(2^8)$. Abbiamo visto che, in tale insieme, ogni byte può essere rappresentato come un polinomio di grado (al più) 7. Ricordando che $m(x) = x^8 + x^4 + x^3 + x + 1$ è il polinomio irriducibile discusso a lezione, si calcoli la somma ed il prodotto dei seguenti due byte:

$$x^7 + x^5 + x^3 + 1 \oplus x^6 + x^3 + x^2 + x = x^7 + x^6 + x^5 + x^3 + x$$

$$\begin{array}{r}
 x^{13} + x^{10} + x^8 + \\
 + x^{11} + x^8 + x^7 + x^6 + \\
 + x^9 + x^6 + x^5 + x^4 + \\
 + x^6 + x^3 + x^2 + x = \\
 \\
 = \cancel{x^{13}} + \cancel{x^{11}} + \cancel{x^{10}} + \cancel{x^7} + \cancel{x^6} + \cancel{x^8} + \cancel{x^4} + \cancel{x^3} + \cancel{x^2} + \cancel{x} \\
 \\
 \cancel{x^{13}} + \cancel{x^5} + \cancel{x^8} + \cancel{x^6} + \cancel{x^5} \\
 \cancel{x^{11}} + \cancel{x^4} + \cancel{x^6} + \cancel{x^4} + \cancel{x^5} \\
 \cancel{x^{10}} + \cancel{x^6} + \cancel{x^5} + \cancel{x^3} + \cancel{x^2} \\
 \cancel{x^5} + \cancel{x^3} + \cancel{x^2} + \cancel{x^1} \\
 \cancel{x^8} + \cancel{x^4} + \cancel{x^3} + \cancel{x^1} \\
 \\
 -2 \quad -1 \quad -1 \quad 1
 \end{array}$$

$$\begin{array}{r}
 \cancel{x} + \cancel{x} + \cancel{x} + \cancel{x} + 1 \\
 \hline
 x^2 + x + 1
 \end{array}$$

5. Sia $F : \{0,1\}^k \times \{0,1\}^{\ell+1} \rightarrow \{0,1\}^L$ una funzione pseudocasuale (sicura). Vogliamo utilizzare F per costruire una funzione $G : \{0,1\}^k \times \{0,1\}^{2\ell} \rightarrow \{0,1\}^{2L}$, nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

$G_k(x)$

Sia $x = x_1 \parallel x_2$ // $|x_1| = |x_2| = \ell$

$y_1 \leftarrow F_k(x_1 \parallel 0) \parallel F_k(x_2 \parallel 1)$

$y_2 \leftarrow F_k(\bar{x}_1 \parallel 0) \parallel F_k(\bar{x}_2 \parallel 1)$ // \bar{x}_i indica la stringa complementare di x_i

$y \leftarrow y_1 \oplus y_2$

return y

Dimostrare formalmente che G non è una funzione pseudo-casuale.

$$x \in \{0,1\}^{2\ell} \Rightarrow x = x_1 \parallel x_2$$

$$\begin{aligned}
 G_k(x) &= F_k(x_1 \parallel 0) \parallel F_k(x_2 \parallel 1) \oplus \\
 &\oplus F_k(\bar{x}_1 \parallel 0) \parallel F_k(\bar{x}_2 \parallel 1) = y^1
 \end{aligned}$$

$$\begin{aligned}
 G_k(\bar{x}) &= F_k(\bar{x}_1 \parallel 0) \parallel F_k(\bar{x}_2 \parallel 1) \oplus \\
 &\oplus F_k(x_1 \parallel 0) \parallel F_k(x_2 \parallel 1) = y^0
 \end{aligned}$$

$$y^1 \oplus y^0 = \emptyset$$

FORMALIZZANDO L'AVVERSARIO:

$A(G)$:

$$x \in \{0,1\}^{2\ell} \parallel x_1 \parallel x_2$$

$$y' \leftarrow \text{OPRF}(x_1 || x_2)$$

$$y'' \leftarrow \text{OPRF}(\tilde{x}_1 || \tilde{x}_2)$$

if ($y' == y''$) return 1
else return 0

$$\Pr_n [\text{ESP}^{\text{Pnf}-1}(A) = 1] = 1$$

$$\Pr_n [\text{ESP}^{\text{Pnf}-0}(A) = 1] = \frac{1}{2^{2L}}$$

$$\text{Adv}^\vee(A) = 1 - \frac{1}{2^L} \gg 0$$

5. Sia $F : \{0,1\}^k \times \{0,1\}^{2t} \rightarrow \{0,1\}^t$ una funzione pseudocasuale. Siano inoltre $a, b, c \in \{0,1\}^\ell$ stringhe note. Vogliamo utilizzare F per costruire una funzione $G : \{0,1\}^k \times \{0,1\}^{3t} \rightarrow \{0,1\}^{3t}$, nel seguente modo (il simbolo \parallel denota l'operazione di concatenazione):

```

 $G_k(x)$ 
Sia  $x = x_1 \parallel x_2 \parallel x_3$  //  $|x_1| = |x_2| = |x_3| = \ell$ 
 $y \leftarrow F_k(x_1 \parallel a) \parallel F_k(x_2 \parallel b) \parallel F_k(x_3 \parallel c)$ 
return y

```

Dimostrare formalmente che G non è una funzione pseudo-casuale.

$G_k(x)$:

$x = x_1 \parallel x_2 \parallel x_3$
 $y \leftarrow F_k(x_1 \parallel a) \parallel F_k(x_2 \parallel b) \parallel F_k(x_3 \parallel c)$
return y

UTILIZZARE LA TECNICA "MIX AND MATCH"

$A(G)$:

$x \in \{0,1\}^{3t}$ // $x = x_1 \parallel x_2 \parallel x_3$
 $z = x_3 \parallel x_2 \parallel x_1$
 $y \leftarrow \text{OPRF}(x)$
 $y'' \leftarrow \text{OPRF}(z)$
if ($x_2^y = x_2^{y''}$) return 1
else return 0

$$\Pr[E_{Sp}^{Pnf-1}(A)] = 1$$

$$\Pr[E_{Sp}^{Pnf-0}(A)] = \frac{1}{2^t}$$

Esercizi Libro

lunedì 15 novembre 2021 22:08

Problem 2.1 Suppose that you want to encrypt a single message $M \in \{0, 1, 2\}$ using a random shared key $K \in \{0, 1, 2\}$. Suppose you do this by representing K and M using two bits (00, 01, or 10), and then XORing the two representations. Does this seem like a good protocol to you? Explain. ■

$$m \in \{0, 1, 2\} \quad k \in \{0, 1, 2\}$$

$$m \in \{0, 1\}^2 \quad k \in \{0, 1\}^2$$

$$c = m \oplus k$$

$$c \in \{0, 1\}^2$$

$$\Pr[E_{\text{enc}_k}(m_1) = c] = \Pr[E_{\text{enc}_k}(m_2) = c]$$

QUESTO RAPPRESENTA UN PROTOCOLLO SICURO

Problem 3.4 As with AES, suppose we are working in the finite field with 2^8 elements, representing field points using the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Compute the byte that is the result of multiplying bytes:

$$\{e1\} \cdot \{05\}$$

$$11100001$$

$$00000101$$

$$(x^7 + x^6 + x^5 + 1) \cdot (x^2 + 1)$$

$$x^9 + x^7 + x^8 + x^6 + x^7 + x^5 + x^2 + 1 =$$

$$= x^9 + x^8 + x^6 + x^5 + x^4 + 1 \quad | \underbrace{x^8 + x^4 + x^3 + x + 1}_{x+1}$$

$$\cancel{x^9} + \cancel{x^8} + x^4 + \cancel{x^2} + x \quad | x+1$$

$$x^8 + x^6 + x^4 + x + 1$$

$$\cancel{x^8} + x^6 + \cancel{x^4} + \cancel{x} + 1$$

$$\begin{array}{r} \cancel{x^8} + \cancel{x^4} + \cancel{x} \\ \hline x^6 + x^3 \end{array}$$

Teoria

lunedì 15 novembre 2021 21:57

DEFINIZIONE DI PERFETTA SICUREZZA

SIA $SE = (KeyGen, Enc, Dec)$ UNO SCHEMA DI CIFRATURA SIMMETRICA E SUPPONIAMO DI USARLO PER CIFRARE MESSAGGI.
AI TRE ALGORITMI DI SE ASSOCIAMO TRE INSIEMI CHE SONO:

- K L'INSIEME DELLE CHIAVI
- M L'INSIEME DEI MESSAGGI
- C L'INSIEME DEI CRIPTOTESTI

DIREMO CHE IL CIFRARIO SE GARANTISCE PERFETTA SICUREZZA SE $\forall m_1, m_2 \in M$ e $\forall c \in C$ SI HA CHE:

$$\Pr[Enc_K(m_1) = c] = \Pr[Enc_K(m_2) = c]$$

DEFINIZIONE PRF

SIA $F: K \times D \rightarrow R$ UNA FAMIGLIA DI FUNZIONI E SIA A UN ALGORITMO CHE USA COME ORACOLO UNA FUNZIONE $g: D \rightarrow R$ E RESTITUISCE UN BIT. CONSIDERIAMO I SEGUENTI ESPERIMENTI

$\text{ESP}_F^{\text{prf-l}}(A)$:

$$K \xleftarrow{R} \mathbb{K}$$

$$b \leftarrow A^{F_K}$$

return b

$\text{ESP}_F^{\text{prf-o}}(A)$:

$$g \xleftarrow{R} \text{FUNC}(D, R)$$

$$b \leftarrow A^g$$

return b

IL PRIMO ESPERIMENTO (A SINISTRA)
 SCEGLIE UN'ISTANZA CASUALE F_k DELLA
 FAMIGLIA \mathcal{F} E QUINDI L'AVVERSARIO A
 USA UN ORACOLO $g = F_k$, CON IL QUALE
 INTERAGISCE INTERROGANDOLO E OTTENENDO
 RISPOSTE, ALLA FINE RITORNERÀ UN bit

IL SECONDO ESPERIMENTO (A DESTRA)
 SCEGLIE UNA FUNZIONE CASUALE $g \in \text{Func}(D, R)$
 DVE $\text{Func}(D, R)$ È L'INSIEME DI TUTTE LE
 FUNZIONI CHE MAPPANO D A R , DOVE LA NERA
 CHIAVE È LA DESCRIZIONE DELLA FUNZIONE.

$$\text{Adv}_F^{\text{Prf}}(A) = |\Pr[\text{Espr}_F^{\text{Prf-1}}(A) = 1] - \Pr[\text{Espr}_F^{\text{Prf-0}}(A) = 1]|$$

DIREMO CHE UNA PRF È SICURA SE
 PER OGNI AVVERSARIO A SI HA CHE:

$$\text{Adv}_F^{\text{Prf}}(A) \approx 0$$

PER OGNI AVVERSARIO POLINOMICAMENTE
 LIMITATO