

Corso di Crittografia

Esercizi Addizionali su Cifrari Simmetrici e MAC

1. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0,1\}^{L+1}$. L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
  if ( $|M| \neq L + 1$ ) return  $\perp$ 
   $r \leftarrow_R \{0,1\}^\ell$ 
  Sia  $m = m_1m_2\dots m_Lm_{L+1}$ 
   $y \leftarrow F_k(r) \oplus (m_1m_2\dots m_L)$ 
   $c \leftarrow y||m_{n+1}$ 
  return  $(c, r)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(c, r)
  if ( $|c| \neq L + 1$ ) return  $\perp$ 
  Sia  $y$  la stringa composta dai primi  $L$  bit di  $c$ 
   $M \leftarrow (y \oplus F_k(r))||c_{L+1}$ 
  return  $M$ 
```

E' questo metodo sicuro? Giustificare la risposta fornita.

2. Sia $F : \{0,1\}^k \times \{0,1\}^{\lambda\ell} \rightarrow \{0,1\}^L$ una funzione pseudocasuale e H una funzione hash resistente alle collisioni il cui insieme dei valori è $\{0,1\}^L$. Si consideri il seguente schema MAC $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $t\ell$, per $0 \leq t \leq \lambda$.

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo **MAC** è definito come segue:

```

MACk( $M$ )
  if ( $|M| \bmod \ell \neq 0$  or  $|M| > \ell\lambda$ ) return  $\perp$ 
   $k' \leftarrow_R F_k(|M|)$ 
  Let  $M = M_1 \cdots M_n$  (con  $|M_i| = \ell$ )
  for  $i = 1$  to  $n$ 
     $y_i \leftarrow F_k(M_i) \oplus H(M_i)$ 
   $Tag \leftarrow y_1 || \dots || y_n$ 
  Return  $Tag$ 

```

Dimostrare che tale schema non e' sicuro.

3. Sia $F : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0, 1\}^L$. L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```

Enck( $M$ )
  if ( $|M| \neq L$ ) return  $\perp$ 
  if ( $M \bmod 2 == 0$ )  $IV \leftarrow 0^\ell$ 
  else  $IV \leftarrow 1^\ell$ 
   $c \leftarrow M \oplus F_k(IV)$ 
  return  $(c, IV)$ 

```

l'algoritmo di decifratura corrispondente è

```

Deck( $c, IV$ )
  if ( $|c| \neq L$ ) return  $\perp$ 
   $M \leftarrow c \oplus F_k(IV)$ 
  return  $M$ 

```

E' questo metodo sicuro? Giustificare la risposta fornita.

4. Sia $F : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente schema MAC (probabilistico) $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $t\ell$ ($t \geq 1$).

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo **MAC** è definito come segue:

```

MACk( $M$ )
  if ( $|M| \bmod \ell \neq 0$ ) return  $\perp$ 
  Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
   $r \leftarrow_R \{0, 1\}^\ell$ 
   $Tag \leftarrow F_k(r) \oplus F_k(M[1]) \oplus \dots \oplus F_k(M[n])$ 
  Return  $(r, Tag)$ 

```

L'algoritmo di verifica funziona nel seguente modo

```
Verk( $M, (r, Tag)$ )
  if ( $|M| \bmod \ell \neq 0$ ) return  $\perp$ 
  Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
   $T \leftarrow F_k(r) \oplus F_k(M[1]) \oplus \cdots \oplus F_k(M[n])$ 
  if Return  $T = Tag$  return 1
  else return 0
```

E' questo metodo sicuro? Giustificare formalmente la risposta fornita.

5. Sia $F : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente schema MAC (deterministico e senza stati) $\Pi = (\text{KeyGen}, \text{MAC})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $t\ell$ (t arbitrario ma tale che $t > 2$).

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```
MACk( $M$ )
  if ( $|M| \bmod \ell \neq 0 \vee |M| < 2\ell$ ) return  $\perp$ 
  Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
  for  $i = 1, \dots, n$   $y_i \leftarrow F_k(M[i])$ 
   $Tag \leftarrow y_1 || y_n$ 
  Return  $Tag$ 
```

E' questo metodo sicuro? Giustificare formalmente la risposta fornita.

6. Sia $F : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente schema MAC, $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza 2ℓ .

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```
MACk( $M$ )
  if ( $|M| \neq (2\ell)$ ) return  $\perp$ 
  Sia  $M = M[0] || M[1]$  //  $|M[i]| = \ell$ 
   $Tag \leftarrow F_k(M[0]) || F_k(\overline{M[1]})$  //  $\overline{M[1]}$  indica il complementare di  $M[1]$ 
  Return  $Tag$ 
```

Dimostrare che il metodo proposto non è sicuro.

1. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0,1\}^{L+1}$. L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
  if ( $|M| \neq L + 1$ ) return  $\perp$ 
   $r \leftarrow_R \{0,1\}^\ell$ 
  Sia  $m = m_1m_2\dots m_Lm_{L+1}$ 
   $y \leftarrow F_k(r) \oplus (m_1m_2\dots m_L)$ 
   $c \leftarrow y||m_{n+1}$ 
  return  $(c, r)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(c, r)
  if ( $|c| \neq L + 1$ ) return  $\perp$ 
  Sia  $y$  la stringa composta dai primi  $L$  bit di  $c$ 
   $M \leftarrow (y \oplus F_k(r))||c_{L+1}$ 
  return  $M$ 
```

E' questo metodo sicuro? Giustificare la risposta fornita.

SI HA UN AVVERSARIO A CHE HA ACCESSO
BLACK BOX ALL'ORAColo DI CIFRATURA LR

PASSIAMO OSSERVARE CHE $m_{L+1} = c_{L+1}$ QUINDI
SI CONSIDERI $x \in \{0,1\}^L$ E SIANO:

$$x_0 = x||0$$

$$x_1 = x||1$$

NEL MOMENTO IN CUI CIFRIAMO $\text{Enc}_k(x_0)$ SI HA:

$$m = x_0^1 x_0^2 \dots x_0^L x_0^{L+1}$$

$$y \leftarrow F_k(r) \oplus m$$

$$c \leftarrow y||x_0^{L+1}$$

LA STESSA COSA SI OTTIENE CON $\text{Enc}_k(x_1)$:

$$c'' \leftarrow y||x_1^{L+1}$$

L'AVVERSARIO PUÒ EFFETTUARE IL SEGUENTE
CONTROLLO: SE C_{L+1} È UGUALI A X_1^{L+1} ALLORA
L'AVVERSARIO SI TROVA NEL MONDO 1, ALTRIMENTI
NEL MONDO 0.

DEFINIAMO FORMALMENTE TALE AVVERSARIO:

A(SE) :

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

$$X_0 = X \| 0$$

$$X_1 = X \| 1$$

$$C \leftarrow O_{ENC}(X_0, X_1)$$

if ($C_{L+1} == 1$) return 1
else return 0

$$\Pr[\text{Esp}^{\text{ind-CPA-1}}(A) = 1] = 1 \xrightarrow{\text{QUESTO COMPORTAMENTO È INDIPENDENTE DALLA CHIAVE SCELTA}}$$

$$\Pr[\text{Esp}^{\text{ind-CPA-0}}(A) = 1] = 0$$

$$\text{Adv}^{\text{ind-CPA}}(A) = |1 - 0| = 1$$

ABBIAMO DIMOSTRATO CHE QUESTO METODO
NON È SICURO!

2. Sia $F : \{0,1\}^k \times \{0,1\}^{\lambda\ell} \rightarrow \{0,1\}^L$ una funzione pseudocasuale e H una funzione hash resistente alle collisioni il cui insieme dei valori è $\{0,1\}^L$. Si consideri il seguente schema MAC II = (KeyGen, MAC, Ver).

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $t\ell$, per $0 \leq t \leq \lambda$.

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```

MACk(M)
  if ( $|M| \bmod \ell \neq 0$  or  $|M| > \ell\lambda$ ) return ⊥
   $k' \leftarrow_R F_k(|M|)$ 
  Let  $M = M_1 \cdots M_n$  (con  $|M_i| = \ell$ )
  for  $i = 1$  to  $n$ 
     $y_i \leftarrow F_k(M_i) \oplus H(M_i)$ 
   $Tag \leftarrow y_1 || \dots || y_n$ 
  Return  $Tag$ 

```

Dimostrare che tale schema non è sicuro.

$$M = \{0,1\}^{t\ell} \quad 0 \leq t \leq \lambda$$

CONSIDERIAMO $x, y \in M$ E SI HA $z = x \parallel y$
 LA CARDINALITÀ DI z È SICURAMENTE UN MULTIPLO
 DI ℓ E SARÀ MAGGIORE DI $\ell\lambda$.

A QUESTO PUNTO SI HA:

$$y_0 = F_k(x) \oplus H(x)$$

$$y_1 = F_k(y) \oplus H(y)$$

$$\text{Tag}' \leftarrow y_0 \parallel y_1$$

L'AVVERSARIO PUÒ CONSIDERARE $w = y \parallel x$
 PER CUI SI HA:

$$\text{Tag}'' \leftarrow y_1 \parallel y_0$$

DEFINIAMO FORMALMENTE L'AVVERSARIO:

A(Π):

$$x \leftarrow M$$

$$y \leftarrow M$$

$$z \leftarrow x || y$$

$$\begin{aligned} \text{Tag}' &\leftarrow O_{\text{MAC}}(z) \quad // \quad \text{Tag}' = y_0 || y_1 = \\ \text{Tag}'' &\leftarrow y_1 || y_0 \\ w &\leftarrow y || z \end{aligned}$$

$$\begin{aligned} &= F_k(x) \oplus H(x) || \\ &F_k(y) \oplus H(y) \end{aligned}$$

$$d \leftarrow \text{VF}_k(w, \text{Tag}'')$$

$$\Pr[\text{Esp}_{\Pi}^{\text{uf-cma}}(A) = 1] = 1$$

QUINDI:

$$\text{Adv}_{\Pi}^{\text{uf-cma}}(A) = 1$$

LO SCHEMA NON È SICURO!

3. Sia $F : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0, 1\}^L$. L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
  if ( $|M| \neq L$ ) return  $\perp$ 
  if ( $M \bmod 2 == 0$ ) IV  $\leftarrow 0^\ell$ 
  else IV  $\leftarrow 1^\ell$ 
  c  $\leftarrow M \oplus F_k(IV)$ 
  return (c, IV)
```

l'algoritmo di decifratura corrispondente è

```
Deck(c, IV)
  if ( $|c| \neq L$ ) return  $\perp$ 
  M  $\leftarrow c \oplus F_k(IV)$ 
  return M
```

E' questo metodo sicuro? Giustificare la risposta fornita.

SI CONSIDERI $x \in \{0, 1\}^{L-1}$ PER CUI SI HA
 $m_0 = x||0$ E $m_1 = x||1$. $|m_0| = |m_1| = L$
 QUINDI ENTRAMBE LE STRINGHE POSSANO ESSERE
 CIFRATE. L'AVVERSARIO FARÀ I SEGUENTI PASSI:

- USA L'ORACOLO UNA PRIMA VOLTA PASSANDO m_0, m_1 PER CUI OTTIENE $C' \leftarrow \text{Enc}(m_0, m_1)$;
- USA L'ORACOLO UNA SECONDA VOLTA PASSANDO m_1, m_2 PER CUI OTTIENE $C'' \leftarrow \text{Enc}(m_1, m_2)$;

ALLORA:

$C = (c, IV)$; $c = M \oplus F_k(IV)$
 SE $IV = 1^\ell$, M È DISPARI QUINDI $M = m_1$,
 ALTRIMENTI SE $IV = 0^\ell$, M È PARI QUINDI $M = m_0$
 QUINDI SE $C' = C''$ VUOL DIRE CHE L'AVVERSARIO
 SI TROVA NEL MONDO 1, ALTRIMENTI NEL MONDO
 0.

DEFINIAMO FORMALMENTE L'AVVERSARIO:

$A(E)$:

$$\times \leftarrow \mathcal{B} \{0, 1\}^{L-1}$$

$$m_0 = \times || 0$$

$$m_1 = \times || 1$$

$$(C', IV') = O_{ENC}(m_0, m_1)$$

$$(C'', IV'') = O_{ENC}(m_2, m_1)$$

if ($IV' == IV''$) return 1

else return 0

$$\Pr [E_{SP_E}^{\text{ind-CPA-1}}(A) = 1] = 1$$

$$\Pr [E_{SP_E}^{\text{ind-CPA-0}}(A) = 0] = 0$$

$$\text{Adv}_E^{\text{ind-CPA}}(A) = 1$$

4. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente schema MAC (probabilistico) $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $t\ell$ ($t \geq 1$).

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```
MACk(M)
  if ( $|M| \bmod \ell \neq 0$ ) return  $\perp$ 
  Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
   $r \leftarrow_R \{0,1\}^\ell$ 
   $\text{Tag} \leftarrow F_k(r) \oplus F_k(M[1]) \oplus \cdots \oplus F_k(M[n])$ 
  Return  $(r, \text{Tag})$ 
```

L'algoritmo di verifica funziona nel seguente modo

```
Verk(M, (r, Tag))
  if ( $|M| \bmod \ell \neq 0$ ) return  $\perp$ 
  Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
   $T \leftarrow F_k(r) \oplus F_k(M[1]) \oplus \cdots \oplus F_k(M[n])$ 
  if Return  $T = \text{Tag}$  return 1
  else return 0
```

E' questo metodo sicuro? Giustificare formalmente la risposta fornita.

SI CONSIDERINO $m_0, m_1 \in \{0, 1\}^\ell$ E SI EFFETTUINO I SEGUENTI PASSI:

- $\Pi = m_0 \parallel m_1$
- $\text{MAC}_k(\Pi) = F_k(r) \oplus F_k(m_0) \oplus F_k(m_1) = (r, \overline{\text{Tag}})$

A QUESTO PUNTO È POSSIBILE CONSIDERARE $\Pi' = m_1 \parallel m_0$ IL CUI $\text{Tag}' = \overline{\text{Tag}}$ INFATTI:

$\text{Ver}_k(\Pi', (r, \overline{\text{Tag}}')) = 1$

SI DEFINISCE L'AVVERSARIO FORMALMENTE:
 $A(\Pi)$:

$m_0, m_1 \xleftarrow{R} \{0, 1\}^\ell$

$\Pi = m_0 \parallel m_1$

$\overline{\text{Tag}} = O_\Pi(\Pi) \parallel \text{Tag} = (r, \overline{\text{tag}})$

$\text{Ver}_k(m_1 \parallel m_0, \overline{\text{Tag}}')$

$\boxed{\Pr_{\Pi}(\text{Esp}_\Pi^{\text{inf-Cma}}(A) = 1) = 1}$
 $\boxed{\text{Adv}(A) = 1}$

LO SCHEMA
NON È SICURO!

5. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente schema MAC (deterministico e senza stati) $\Pi = (\text{KeyGen}, \text{MAC})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $t\ell$ (t arbitrario ma tale che $t > 2$).

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

$\text{MAC}_k(M)$

```

if ( $|M| \bmod \ell \neq 0 \vee |M| < 2\ell$ ) return ⊥
Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
for  $i = 1, \dots, n$   $y_i \leftarrow F_k(M[i])$ 
 $Tag \leftarrow y_1 || y_n$ 
Return  $Tag$ 

```

E' questo metodo sicuro? Giustificare formalmente la risposta fornita.

$$M \in \{0,1\}^{t\ell}, t > 2$$

SI CONSIDERI $m \in \{0,1\}^{t\ell}$ PER CUI SI HA CHE
 $|m| \bmod \ell = 0$ E $|m| > 2\ell$ QUINDI m
 RAPPRESENTA UNA STRINGA VALIDA.

SIA $X = m[1] \dots m[n]$ CON $|m[i]| = \ell$.

SIA $y_i = F_k(m[i])$ PER $i = 1, \dots, n$

$$\text{ALLORA } Tag = y_1 || y_m$$

A QUESTO PUNTO È POSSIBILE CONSIDERARE
 $x' = m[m] m[2] \dots m[m-1] m[1]$

$$\text{ALLORA } Tag' = y_m || y_1$$

SI DEFINISCE FORMALMENTE L'AVVERSARIO:

$A(\Pi)$:

$$m \xleftarrow{R} \{0,1\}^{t\ell}$$

$$X = m[1] \dots m[m]$$

$$Tag = O_\Pi(X) // Tag' = y_1 || y_m$$

$$x' = m[m] m[2] \dots m[m-1] m[1]$$

$$VF_k(x', y_m || y_1)$$

$$\Pr[\text{ESP}_{\pi}^{\text{uf-cma}}(A) = 1] = 1$$

$$\text{Adv}_{\pi}^{\text{uf-cma}}(A) = 1$$

Lo SCHEMA NON È SICURO!

6. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente schema MAC, $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza 2ℓ .

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```

 $\text{MAC}_k(M)$ 
if ( $|M| \neq (2\ell)$ ) return  $\perp$ 
Sia  $M = M[0]||M[1]$  //  $|M[i]| = \ell$ 
 $\text{Tag} \leftarrow F_k(M[0])||F_k(\overline{M[1]})$  //  $\overline{M[1]}$  indica il complementare di  $M[1]$ 
Return  $\text{Tag}$ 

```

Dimostrare che il metodo proposto non è sicuro.

$M = \{0,1\}^{2\ell}$ SPAZIO DEI MESSAGGI, CONSIDERIAMO
 $m_1 = X||X$ con $X \in \{0,1\}^\ell$

PER TALE INPUT SI HA:

$$\text{Tag}_1 = F_k(X) || F_k(\overline{X})$$

$$m_2 = Y||Y \text{ con } Y \in \{0,1\}^\ell$$

PER TALE INPUT SI HA:

$$\text{Tag}_2 = F_k(Y) || F_k(\overline{Y})$$

QUINDI POSSO CONSIDERARE $m_3 = X||Y$, IC CUI Tag_3 SARÀ:

$$\begin{array}{c} F_k(X) || F_k(\overline{Y}) \\ \Downarrow \quad \Downarrow \\ \text{Tag}_1[0] || \text{Tag}_2[1] \end{array}$$

FORMALIZZIAMO L'AVVERSARIO:

$A(\Pi_A)$:

$$X, Y \xleftarrow{R} \{0,1\}^\ell$$

$$\text{Tag}_1 \leftarrow O_{\Pi_A}(X||X)$$

$$\text{Tag}_2 \leftarrow O_{\Pi_A}(Y||Y)$$

$$O_{\nabla F}(X||Y, \text{Tag}_1[0]||\text{Tag}_2[1])$$

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

$$\text{Adv}^{\text{uf-cma}}(A) = 1$$

Corso di Crittografia

Prova in Itinere del 24 Maggio 2013

1. Definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a messaggio scelto) per cifrari simmetrici.
2. Sia $E : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ un cifrario a blocchi sicuro e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0, 1\}^{2\ell}$. L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
  if ( $|M| \neq 2\ell \vee |M| == 0$ ) return  $\perp$ 
  Sia  $M = M_1 || M_2 \text{ // } |M_i| = \ell$ , e  $||$  indica concatenazione
   $r \leftarrow_R \{0, 1\}^\ell$ 
   $c_1 \leftarrow E_k(r) \oplus M_1;$ 
   $c_2 \leftarrow r \oplus M_2;$ 
   $c \leftarrow c_1 || c_2$ 
  return  $(r, c)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(r, c)
  if ( $|c| \neq 2\ell \vee |c| == 0$ ) return  $\perp$ 
  Sia  $c = c_1 || c_2$ 
   $M_1 \leftarrow E_k(r) \oplus c_1; M_2 \leftarrow c_2 \oplus r$ 
   $M \leftarrow M_1 || M_2$ 
  return  $M$ 
```

Dimostrare che tale cifrario non è sicuro in senso IND-CPA.

3. (a) Si definisca il concetto di funzione hash resistente alle collisioni ($\text{cr2} - \text{kk}$).
(b) Si dimostri che la seguente funzione hash H non è resistente alle collisioni.
Lo spazio degli input ammissibili è $D = \{0, 1\}^{t\ell}$ $t \geq 1$. Sia $F : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ una funzione pseudocasuale. Sia inoltre $k \in \{0, 1\}^n$ una chiave pubblicamente nota. H è definita come segue

```

H( $M$ )
  if ( $|M| \bmod \ell \neq 0$ ) return  $\perp$ 
  Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
   $y \leftarrow \bigoplus_{i=1}^t F_k(M[i])$ 
  Return  $y$ 

```

4. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per MAC.
5. Siano $F_1 : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ e $F_2 : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ due funzioni pseudocasuali e si consideri il seguente schema MAC $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza 2ℓ .

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di $2n$ bit. L'algoritmo MAC è definito come segue:

```

MAC $k$ ( $M$ )
  if ( $|M| \neq 2\ell$ ) return  $\perp$ 
  Sia  $k = k_1 || k_2$  //  $|k_i| = n$ 
  Sia  $M = M_1 || M_2$  //  $|M[i]| = \ell$ 
   $Tag \leftarrow (F_{k_1}(M_1) \oplus F_{k_1}(\bar{M}_2)) || (F_{k_2}(M_1) \oplus (F_{k_2}(\bar{M}_2)))$  //  $\bar{M} = M \oplus 1^\ell$ 
  Return  $Tag$ 

```

Dimostrare che tale schema non è sicuro.

1. Definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a messaggio scelto) per cifrari simmetrici.

Sia $SE = (\text{KeyGen}, \text{Enc}, \text{Dec})$ un cifrario simmetrico e sia A un avversario che ha accesso ad un oracolo che dà il messaggio ℓ destro o sinistra in base al valore di un bit b . Questo viene chiamato lr-encryption oracle indicato con $\text{Enc}_K(\text{LR}(\cdot, \cdot, b))$. La funzione LR è così definita:

$$\text{LR}(x_0, x_1, b) = \begin{cases} x_0 & \text{se } b=0 \\ x_1 & \text{se } b=1 \end{cases}$$

Si considerino i seguenti esperimenti:

$\text{ESP}_{\text{SE}}^{\text{ind-CPA-1}}(A)$:

$K \leftarrow \mathbb{K}$
 $d \leftarrow A^{\text{Enc}_K(\text{LR}(\cdot, \cdot, 1))}$
return d

$\text{ESP}_{\text{SE}}^{\text{ind-CPA-0}}(A)$:

$K \leftarrow \mathbb{K}$
 $d \leftarrow A^{\text{Enc}_K(\text{LR}(\cdot, \cdot, 0))}$
return d

L'obiettivo dell'avversario è quello di sapere se si trova nel mondo 1, ovvero l'oracolo restituisce la cifratura del messaggio destro, oppure si trova nel mondo 0, ovvero l'oracolo restituisce la cifratura del messaggio sinistro.

Per fare ciò l'avversario può fare delle richieste all'oracolo del tipo (M_0, M_1) con $|M_0| = |M_1|$.

Il vantaggio dell'avversario IND-CPA è definito come segue:

$$\text{Adv}^{\text{ind-CPA}}(A) = |\Pr[\text{ESP}_{\text{SE}}^{\text{ind-CPA-1}}(A) = 1] - \Pr[\text{ESP}_{\text{SE}}^{\text{ind-CPA-0}}(A) = 1]|$$

Diciamo che SE è un cifrario simmetrico che fornisce indistinguibilità relativamente ad attacchi a testa in chiave se il $\text{Adv}^{\text{ind-CPA}}(A)$ è prossimo a ZERO & A p. l.

2. Sia $E : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ un cifrario a blocchi sicuro e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0,1\}^{2\ell}$. L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
if ( $|M| \neq 2\ell \vee |M| == 0$ ) return  $\perp$ 
Sia  $M = M_1||M_2 // |M_i| = \ell$ ,  $e //$  indica concatenazione
 $r \leftarrow_R \{0,1\}^\ell$ 
 $c_1 \leftarrow E_k(r) \oplus M_1;$ 
 $c_2 \leftarrow r \oplus M_2;$ 
 $c \leftarrow c_1||c_2$ 
return  $(r, c)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(r, c)
if ( $|c| \neq 2\ell \vee |c| == 0$ ) return  $\perp$ 
Sia  $c = c_1||c_2$ 
 $M_1 \leftarrow E_k(r) \oplus c_1; M_2 \leftarrow c_2 \oplus r$ 
 $M \leftarrow M_1||M_2$ 
return  $M$ 
```

Dimostrare che tale cifrario non è sicuro in senso IND-CPA.

$M = \{0,1\}^{2\ell}$ CONSIDERIAMO $m_0 = X||X$ con $X \in \{0,1\}^\ell$

PER TALE INPUT SI HA:

$$c_1 \leftarrow E_k(r) \oplus X$$

$$c_2 \leftarrow r \oplus X$$

$$c \leftarrow c_1||c_2 = E_k(r) \oplus X||r \oplus X$$

$$\text{return } (r, c)$$

$$m_1 = X||Y \text{ con } Y \in \{0,1\}^\ell$$

$$c_1 \leftarrow E_k(r) \oplus X$$

$$c_2 \leftarrow r \oplus Y$$

$$c \leftarrow c_1||c_2 = E_k(r) \oplus X||r \oplus Y$$

CONSIDERIAMO $X = 0^\ell$ E $Y = 1^\ell$ ALLORA

$$c \leftarrow c_1||c_2 = E_k(r) \oplus \boxed{r} \rightarrow \text{l'avversario conosce } r$$

$$c'' \leftarrow c_1||c_2 = E_k(r) \oplus r \oplus 1^\ell$$

$A(Se) :$

$$X = 0^l$$

$$Y = 1^l$$

$$m_0 = X \parallel X$$

$$m_1 = X \parallel Y$$

$$(r, c_1 \parallel c_2) = O_{enc}(m_0, m_1)$$

if ($c_2 \neq r$) return 1

else return 0

$$\Pr_n [ESP^{ind-CPA-1}(A) = 1] = 1$$

$$\Pr_n [ESP^{ind-CPA-0}(A) = 1] = 0$$

$$\text{Adv}_r^{ind-CPA}(A) = 1 - 0 = 1$$

3. (a) Si definisca il concetto di funzione hash resistente alle collisioni (cr2 - kk).

Sia $H : K \times D \rightarrow R$ una famiglia di funzioni hash e sia A un avversario contro la resistenza alle collisioni (CR2-KK). Consideriamo il seguente esperimento:

$\text{ESP}_H^{\text{cr2-uu}}$ (H):

$K \leftarrow K$; $(x_1, x_2) \leftarrow A(K)$;

$\text{if } H_K(x_1) = H_K(x_2) \wedge x_1 \neq x_2 \wedge x_1, x_2 \in D$)

return 1

else

return 0

In questo esperimento l'avversario conosce la chiave K e in base a quella tenta di generare x_1 e x_2 tale che $H(x_1) = H(x_2)$ $\wedge x_1 \neq x_2 \wedge x_1, x_2 \in D$, se questo accade l'esperimento tornerà 1, altrimenti 0. Il vantaggio dell'avversario CR2-KK è definito come segue:

$$\text{Adv}^{\text{cr2-uu}}(A) = \Pr[\text{ESP}_H^{\text{cr2-uu}}(A) = 1]$$

che dipende dalla probabilità di 1 nel generare x_1 e x_2 .

Diremo che H è una famiglia di funzioni resistente alle collisioni se $\text{Adv}^{\text{cr2-uu}}(A) \approx 0 \forall A$ p.l.

Si dimostri che la seguente funzione hash H non è resistente alle collisioni.
 Lo spazio degli input ammissibili è $D = \{0, 1\}^{t\ell}$ $t \geq 1$. Sia $F : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ una funzione pseudocasuale. Sia inoltre $k \in \{0, 1\}^n$ una chiave pubblicamente nota. H è definita come segue

```
H(M)
    if ( $|M| \bmod \ell \neq 0$ ) return  $\perp$ 
    Sia  $M = M[1] \cdots M[n]$  //  $|M[i]| = \ell$ 
     $y \leftarrow \bigoplus_{i=1}^t F_k(M[i])$ 
    Return  $y$ 
```

CONSIDERO $X, Y \in \{0, 1\}^\ell$ PER CUI $m_0 = X \parallel Y$

$$H(m_0) = F_k(X) \oplus F_k(Y)$$

CONSIDERO $m_1 = Y \parallel X$

$$H(m_1) = F_k(Y) \oplus F_k(X)$$

OSSERVIAHO CHE $H(m_0) = H(m_1)$, $m_0 \neq m_1$, $m_0, m_1 \in D$

$A(H)$:

$$X, Y \xleftarrow{R} \{0, 1\}^\ell // X \neq Y$$

$$m_0 \leftarrow X \parallel Y$$

$$m_1 \leftarrow Y \parallel X$$

$$\text{return } (m_0, m_1)$$

$$\Pr[\text{Esp}^{Cn^2 - \kappa n}(A) = 1] = 1$$

$$\text{Adv}^{Cn^2 - \kappa n}(A) = 1$$

4. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per MAC.

Sia $\text{MAC}: K \times \{0,1\}^* \rightarrow \{0,1\}^*$ un codice di autenticazione del messaggio e sia A un avversario contro la falsificabilità del messaggio in chiave che ha accesso ad un oracolo di firma e un oracolo di verifica.

Si considera il seguente esperimento:

$\text{ESP}_{\text{MAC}}^{\text{uf-ema}}(A)$:

$K \xleftarrow{R} \text{KeyGen}()$

Run $A^{K_{\text{MAC}}(\cdot), V_{\text{F}}(\cdot)}$

if A ASKS $V_{\text{F}}(M, \text{tag})$ TALE CHE:

- L'ORACOLO DI VERIFICA RITORNA 1

- A NON AVEVA RICHIESTO M ALL'ORACOLO MAC

Return 1

else return 0

L'avversario effettua un certo numero di richieste all'oracolo MAC, dette chiamate di firma e si indicano con q_s ; ed effettua un altro numero di richieste all'oracolo VF, dette chiamate di verifica e si indicano con q_v . Invia tali richieste senza riuscire a falsificare un messaggio.

Il vantaggio dell'avversario uf-ema è:

$$\text{Adv}^{\text{uf-ema}}(A) = \Pr[\text{ESP}_{\text{MAC}}^{\text{uf-ema}}(A) = 1]$$

Diremo che MAC garantisce la non falsificabilità
dei messaggi a testo chiaro scelta \times $\text{Ad}^{\text{uf-tma}}_{\text{CAI}=0}$
 $\forall A$ p.l.

5. Siano $F_1 : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ e $F_2 : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ due funzioni pseudocasuali e si consideri il seguente schema MAC $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza 2ℓ .

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di $2n$ bit. L'algoritmo **MAC** è definito come segue:

```
MACk(M)
  if ( $|M| \neq 2\ell$ ) return ⊥
  Sia  $k = k_1 || k_2$  //  $|k_i| = n$ 
  Sia  $M = M_1 || M_2$  //  $|M[i]| = \ell$ 
   $Tag \leftarrow (F_{k_1}(M_1) \oplus F_{k_1}(\bar{M}_2)) || (F_{k_2}(M_1) \oplus F_{k_2}(\bar{M}_2))$  //  $\bar{M} = M \oplus 1^\ell$ 
  Return Tag
```

Dimostrare che tale schema non è sicuro.

$$M = \{0,1\}^{2\ell} \quad \text{CONSIDERO } m_0 = X||Y \text{ con } X, Y \in \{0,1\}^\ell$$

$$\text{Tag} = (F_{K_1}(X) \oplus F_{K_1}(\bar{Y})) || (F_{K_2}(X) \oplus F_{K_2}(\bar{Y}))$$

$$m_0 = 0^\ell || 0^\ell$$

$$\text{Tag} = (F_{K_1}(0^\ell) \oplus F_{K_1}(1^\ell)) || (F_{K_2}(0^\ell) \oplus F_{K_2}(1^\ell))$$

$$m_1 = 1^\ell || 1^\ell \quad \text{E} \quad \text{Tag}' = \text{Tag}$$

A(MA) :

$$m_0 = 0^\ell || 0^\ell$$

$$\text{Tag} = O_{\text{MAC}}(m_0)$$

$$m_1 = 1^\ell || 1^\ell$$

$$O_{\text{VF}}(m_1, \text{Tag})$$

$$\text{Ad}v(A) = 1$$

Corso di Crittografia

Prova in Itinere del 20 Maggio 2011

1. Definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a messaggio scelto) per cifrari simmetrici.
2. Sia $E : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ un cifrario a blocchi sicuro e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0,1\}^{2\ell}$. L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
  if ( $|M| \neq 2\ell \vee |M| == 0$ ) return ⊥
  Sia  $M = M_1 ||| M_2 // |M_i| = \ell$ , e  $||$  indica concatenazione
   $r \leftarrow_R \{0,1\}^\ell$ 
   $c_1 \leftarrow E_k(r \oplus M_1); c_2 \leftarrow E_k(M_2)$ 
   $c \leftarrow c_1 || c_2$ 
  return  $(r, c)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(r, c)
  if ( $|c| \neq 2\ell \vee |c| == 0$ ) return ⊥
  Sia  $c = c_1 || c_2$ 
   $M_1 \leftarrow E_k^{-1}(c_1) \oplus r; M_2 \leftarrow E_k^{-1}(c_2)$ 
   $M \leftarrow M_1 || M_2$ 
  return  $M$ 
```

Dimostrare che tale cifrario non è sicuro in senso IND-CPA.

3. In classe abbiamo definito il concetto di funzione universale nel seguente modo.
Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

```
Esperimento EspHcr0-kk(A)
   $(x_1, x_2) \leftarrow A(\cdot);$ 
   $k \leftarrow_R \mathcal{K};$ 
  if ( $H_k(x_1) = H_k(x_2)$ ) and ( $x_1 \neq x_2$ ) and ( $x_1, x_2 \in D$ ) Return 1
  else Return 0
```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{cr0-kk}} = \Pr \left[\mathbf{Esp}_H^{\text{cr0-kk}}(A) = 1 \right]$$

Diciamo che H è una funzione universale se tale vantaggio è piccolo per ogni avversario polinomialmente limitato.

- (a) Si definisca il concetto di funzione universale unidirezionale (cr1-kk).
 - (b) Si dimostri che ogni funzione universale unidirezionale è anche una funzione universale.
4. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per MAC.
5. Siano $F : \{0, 1\}^k \times \{0, 1\}^{\lambda\ell} \rightarrow \{0, 1\}^k$ e $F' : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ due funzioni (dimostrabilmente) pseudocasuali e si consideri il seguente schema MAC $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $t\ell$, per $0 \leq t \leq \lambda$.

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```

MAC $k$ ( $M$ )
  if ( $|M| \bmod \ell \neq 0$  or  $|M| > \ell\lambda$ ) return ⊥
   $k' \leftarrow_R F_k(|M|)$ 
  Let  $M = M_1 \cdots M_n$  (con  $|M_i| = \ell$ )
  for  $i = 1$  to  $n$ 
     $y_i \leftarrow F_{k'}(M_i)$ 
   $Tag \leftarrow y_1 || \dots || y_n$ 
  Return  $Tag$ 

```

Dimostrare che tale schema non è sicuro.

- Definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a messaggio scelto) per cifrari simmetrici.

Sia $SE = (KeyGen, Enc, Dec)$ un cifrario simmetrico e sia A un avversario che ha accesso ad un oracle che prende un input due messaggi M_0, M_1 tale che valga $|M_0| = |M_1|$ e restituisce in output o la riflessione del messaggio di destra (M_2) o la riflessione del messaggio di sinistra (M_0), in base al valore di un bit b . Questo oracle prende il nome di LR -encryption oracle, $\text{Enc}_K(LR(\cdot, \cdot, b))$.

$$LR(x_0, x_1, b) = \begin{cases} x_0 & \text{se } b=0 \\ x_1 & \text{se } b=1 \end{cases}$$

Si considerino i seguenti esperimenti:

$\text{ESP}_{SE}^{\text{ind-CPA-1}}(A)$:

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

$$d \leftarrow \text{Enc}_K(LR(\cdot, \cdot, 1))$$

return d

$\text{ESP}_{SE}^{\text{ind-CPA-0}}(A)$:

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

$$d \leftarrow \text{Enc}_K(LR(\cdot, \cdot, 0))$$

return d

L'obiettivo dell'avversario è quello di capire se si trova nel mondo 1, ovvero dati due messaggi M_1, M_2 con $|M_1| = |M_2|$, l'oracle restituirà all'utente sempre la riflessione del messaggio M_1 . Viceversa per il mondo 0.

Il vantaggio dell'interdizione è definito come:

\text{Adv}^{\text{ind-CPA}}(A) = |\Pr_{\text{SE}}[\text{ESP}_{\text{SE}}^{\text{ind-CPA-1}}(A) = 1] - \Pr_{\text{SE}}[\text{ESP}_{\text{SE}}^{\text{ind-CPA-0}}(A) = 1]|

Diremo che il cifrario SE garantisce indistinguibilità ad attacco a messaggio nascosto se $\text{Adv}^{\text{ind-CPA}}(A) \approx 0$ $\forall A$ p. l.

2. Sia $E : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ un cifrario a blocchi sicuro e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0,1\}^{2\ell}$. L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
  if ( $|M| \neq 2\ell \vee |M| == 0$ ) return  $\perp$ 
  Sia  $M = M_1 || M_2 // |M_i| = \ell$ , e  $\parallel$  indica concatenazione
   $r \leftarrow_R \{0,1\}^\ell$ 
   $c_1 \leftarrow E_k(r \oplus M_1); c_2 \leftarrow E_k(M_2)$ 
   $c \leftarrow c_1 || c_2$ 
  return  $(r, c)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(r, c)
  if ( $|c| \neq 2\ell \vee |c| == 0$ ) return  $\perp$ 
  Sia  $c = c_1 || c_2$ 
   $M_1 \leftarrow E_k^{-1}(c_1) \oplus r; M_2 \leftarrow E_k^{-1}(c_2)$ 
   $M \leftarrow M_1 || M_2$ 
  return  $M$ 
```

Dimostrare che tale cifrario non è sicuro in senso IND-CPA.

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

SI CONSIDERI $M_0 = X || X$ CON $X \in \{0,1\}^\ell$ ALLORA

$$m = X || X$$

$$r \leftarrow_R \{0,1\}^\ell$$

$$C_1 \leftarrow E_k(r \oplus X)$$

$$C_2 \leftarrow E_k(X)$$

$$\text{return}_n(r, C_1 || C_2)$$

SI CONSIDERI $M_1 = X || Y$ CON $Y \in \{0,1\}^\ell$, $X \neq Y$

ALLORA:

$$m = X || Y \quad r \leftarrow_R \{0,1\}^\ell \quad C_1 \leftarrow E_k(r \oplus X)$$

$$C_2 \leftarrow E_k(Y)$$

DEFINIAMO FORMLAMENTE L'AVVERSARIO:

A(SE):

$$x, y \in \{0, 1\}^{\ell} \quad // \quad x \neq y$$

$$m_0 = x \| x$$

$$m_1 = x \| y$$

$$(v, c') \leftarrow O_{ENC}(m_0, m_1) \quad // \quad c' = c'_1 \| c'_2$$

$$(v, c'') \leftarrow O_{ENC}(m_0, m_0) \quad // \quad c'' = c''_1 \| c''_2$$

if ($c'_2 \neq c''_2$) return 1

else return 0

$$\Pr[\text{Esp}_{SE}^{IND-CPA-t}(A) = 1] = 1$$

$$\Pr[\text{Esp}_{SE}^{IND-CPA-0}(A) = 1] = 0$$

$$\text{Adv}^{IND-CPA}(A) = |1 - 0| = 1$$

3. In classe abbiamo definito il concetto di funzione universale nel seguente modo.

Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

Esperimento $\text{Esp}_H^{\text{cr0-kk}}(A)$
 $(x_1, x_2) \leftarrow A(\cdot);$
 $k \leftarrow_R \mathcal{K};$
if $(H_k(x_1) = H_k(x_2))$ and $(x_1 \neq x_2)$ and $(x_1, x_2 \in D)$ Return 1
else Return 0

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{cr0-kk}} = \Pr [\text{Esp}_H^{\text{cr0-kk}}(A) = 1]$$

Diciamo che H è una funzione universale se tale vantaggio è piccolo per ogni avversario polinomialmente limitato.

- (a) Si definisca il concetto di funzione universale unidirezionale (cr1-kk).
- (b) Si dimostri che ogni funzione universale unidirezionale è anche una funzione universale.

(A)

SIA $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia
 A un avversario che ha accesso ad essa.
Si consideri il seguente esperimento:

$\text{Esp}_H^{\text{cr1-kk}}(A)$:

$(x_1, \text{stato}) \leftarrow A();$

$K \leftarrow_R \mathcal{K};$

$x_2 \leftarrow A(K, \text{stato});$

if $(H_K(x_2) == H_K(x_1) \wedge x_1 \neq x_2 \wedge x_1, x_2 \in D)$:

return 1

else return 0

L'avversario A all'inizio non conosce la chiave K e durante la prima esecuzione darà in output un valore casuale $x_1 \in D$ e uno stato per capire che è stato eseguito una prima volta. Per la seconda esecuzione l'avversario ormai

in input la chiave e lo stato e ritorna x_2 , conoscendo la chiave.

Il vantaggio di questo avversario è definito come:

$$\text{Adv}^{\text{CR1-UN}}(A) = \Pr[\text{Esp}_H^{\text{CR2-KR}}(A) = 1]$$

Diciamo che H è una funzione hash unidimensionale unidirezionale se per ogni avversario A polinomialmente limitata, il vantaggio di A CR1-UN è prossimo a ZERO.

(b)

H_p : H è CR1-UN

T_S : H ALLORA È CR0-KR

SUPPONIAMO PER ASSURDO CHE H NON SIA UNA FUNZIONE UNIDIREZIONALE, ALLORA ESISTE B CHE È UN AVVERSARIO CR0-KR IL COI VANTAGGIO, $\text{Adv}^{\text{CR0-KR}}(B)$, È MOLTO MAGGIORRE 0. SI CONSIDERI UN AVVERSARIO A CR1-KR CHE SFRUTTI B E CI PERMETTA DI CONTRADDIRE L'IPOTESI INIZIALE, OWERO CHE H È CR1-KR.

RICORDIAMO CHE A VIENE ESEGUITO 2 VOLTE.

1. $A()$:

$x_1, x_2 \leftarrow B()$

$\text{stato} \leftarrow x_2$

$\text{return}(x_1, \text{stato})$

DURANTE LA PRIMA ESECUZIONE L'AVVERSARIO A SFRUTTA B PER OTTENERE x_2 e x_2 , STATO SARÀ POSTA A x_2 E RITORNERÀ (x_2, stato) , CHE È COERENTE CON CIÒ CHE ABBIATO RISTO NELL'ESPERIMENTO.

2. $A(k, \text{stato})$:

$x_2 \leftarrow \text{stato}$

if ($H_k(x_2) \neq H_k(x_2)$):

return $x_2 \stackrel{R}{\leftarrow} D$

else

return x_2

PER LA SECONDA ESECUZIONE DI A L'AVVERSARIO PRENDE IN INPUT LA CHIAVE E LO STATO, ACCORDA SETTA $x_2 = \text{stato}$, VERIFICA SE x_1 e x_2 PERMETTONO DI OTTENERE UNA COLLISIONE, SE NON È UNA COLLUSIONE, ALLORA RESTITUISCE IN MANIERA RANDOM UN VALORE $x_2 \in D$.

POSSIAMO OSSERVARE CHE:

$$\text{Adv}^{\text{cr1}-KK}(A) \geq \text{Adv}^{\text{cr0}-KK}(B) \gg 0$$

QUESTO È UN ASSURDO DATO CHE AVEVAMO SUPPOSTO CHE H FOSSE UNIDIREZIONALE UNIVERSALE E QUINDI DEVE NECESSARIAMENTE ESSERE ANCHE UNIVERSALE, CHE È LA TESI.

4. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per MAC.

SIA $\text{MA} = (\text{KeyGen}, \text{MAC}, \text{VF})$ UNO SCHEMA DI CODIFICA PER L'AUTORIZZAZIONE DEI MESSAGGI. DOVE:

- KeyGen È L'ALGORITMO DI GENERAZIONE DELLA CHIAVE
- MAC : $K \times \{0,1\}^* \rightarrow \{0,1\}^*$ È UN CODICE DI AUTENTICAZIONE DEL MESSAGGIO
- VF : $K \times \{0,1\}^* \rightarrow \{0,1\}$ È UN ALGORITMO DI VERIFICA PER I TAG.

SIA A UN AVVERSARIO CHE PUÒ ESEGUIRE q_S RICHIESTE AD UN ORACOLO MAC E q_V RICHIESTE AD UN ORACOLO VF.

SI CONSIDERI IL SEGUENTE ESPERIMENTO:

$\text{Esp}_{\text{MA}}^{\text{uf-cma}}(A)$:

```
K ← KeyGen();
RUN AMAC_K(.), VF_K(.)
```

if A FA UNA RICHIESTA DI VERIFICA (M, Tag) TALE CHE:

- L'ORACOLO DI VERIFICA RISPONE 1;
- N NON ERA STATO GIÀ RICHIESTO ALL'ORACOLO MAC;

Return 1

else return 0

L'OBBIETTIVO DELL'AVVERSARIO È QUELLO DI FALSIFICARE UN MESSAGGIO.

IL VANTAGGIO DI TALE AVVERSARIO È:

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

DI REMO CHE HA GARANTISCE LA NON FALSIFICABILITÀ
SE PER OGNI AVVERSAIO POLINOMICAMENTE LIMITATO
 $\text{Adv}_{\pi_A}^{\text{af-ema}}(A) \approx 0$.

5. Siano $F : \{0,1\}^k \times \{0,1\}^{\lambda\ell} \rightarrow \{0,1\}^k$ e $F' : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ due funzioni (dimostrabilmente) pseudocasuali e si consideri il seguente schema MAC $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $t\ell$, per $0 \leq t \leq \lambda$.

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```

 $\text{MAC}_k(M)$ 
  if ( $|M| \bmod \ell \neq 0$  or  $|M| > \ell\lambda$ ) return  $\perp$ 
   $k' \leftarrow_R F_k(|M|)$ 
  Let  $M = M_1 \cdots M_n$  (con  $|M_i| = \ell$ )
  for  $i = 1$  to  $n$ 
     $y_i \leftarrow F_{k'}(M_i)$ 
   $\text{Tag} \leftarrow y_1 || \dots || y_n$ 
  Return  $\text{Tag}$ 
```

Dimostrare che tale schema non è sicuro.

$$M = \{0,1\}^{t\ell} \quad \text{con } 0 \leq t \leq \lambda$$

$$\text{SI CONSIDERI } m_0 = x \quad \text{con } x \in \{0,1\}^\ell$$

$$\text{MAC}_k(m_0) = \text{Tag} = y_1 = F_{k'}(x)$$

$$\text{SI CONSIDERI } m_1 = x || x \quad \text{IC } \text{Tag}' = \text{Tag} || \text{Tag}$$

DEFINIAMO FORMALMENTE L'AVVERSARIO:

$A(\Pi)$:

$$x \leftarrow_R \{0,1\}^\ell$$

$$\text{Tag} \leftarrow \text{Onac}(x)$$

$$\text{Ver}(x || x, \text{Tag} || \text{Tag}')$$

$$\Pr[\text{ES}_{P_{\text{NA}}}^{\text{uf-cma}}(A) = 1] = 1$$

$$\text{Adv}_{P_{\text{NA}}}^{\text{uf-cma}}(A) = 1$$

Corso di Crittografia

Prova in Itinere del 17 Dicembre 2009

1. Definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a crittotesto scelto) per cifrari simmetrici.
2. Sia $E : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ un cifrario a blocchi sicuro e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0, 1\}^{t\ell}$ ($t \geq 2$). L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck( $M$ )
  if ( $|M| \bmod \ell \neq 0 \vee |M| == 0$ ) return  $\perp$ 
  Sia  $M = M_1 \parallel \dots \parallel M_s$  //  $|M_i| = \ell$ , e  $\parallel$  indica concatenazione
   $IV \leftarrow_R \{0, 1\}^\ell$ 
   $c_1 \leftarrow E_k(IV) \oplus M_1$ 
  for  $i = 2, \dots, s$ 
     $c_i \leftarrow E_k(M_i \oplus c_{i-1} \oplus M_{i-1})$ 
  end for
   $c \leftarrow c_1 \parallel \dots \parallel c_s$ 
  return  $(IV, c)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck( $IV, c$ )
  if ( $|c| \bmod \ell \neq 0 \vee |c| == 0$ ) return  $\perp$ 
  Sia  $c = c_1 \parallel \dots \parallel c_s$ 
   $M_1 \leftarrow E_k^{-1}(IV) \oplus c_1$ 
  for  $i = 2, \dots, s$ 
     $M_i \leftarrow E_k^{-1}(c_i) \oplus M_{i-1} \oplus c_{i-1}$ 
  end for
   $M \leftarrow M_1 \parallel \dots \parallel M_s$ 
  return  $M$ 
```

Dimostrare che tale cifrario non è sicuro contro attacchi a crittotesto scelto.

3. In classe abbiamo definito il concetto di funzione universale nel seguente modo.

Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

```
Esperimento  $\text{Esp}_H^{\text{cr0-kk}}(A)$ 
   $(x_1, x_2) \leftarrow A(\cdot);$ 
   $k \leftarrow_R \mathcal{K};$ 
  if ( $H_k(x_1) = H_k(x_2)$ ) and ( $x_1 \neq x_2$ ) and ( $x_1, x_2 \in D$ ) Return 1
  else Return 0
```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{cr0-kk}} = \Pr [\text{Esp}_H^{\text{cr0-kk}}(A) = 1]$$

Diciamo che H è una funzione universale se tale vantaggio è piccolo per ogni avversario polinomialmente limitato.

- (a) Si definisca il concetto di funzione resistente alle collisioni (cr2 - kk).
 - (b) Si dimostri che ogni funzione resistente alle collisioni è anche una funzione universale.
4. In classe abbiamo studiato il paradigma PRF-as-a-MAC. Si consideri la seguente variante (randomizzata) del metodo. Sia $F : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente schema MAC $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza ℓ .

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```
 $\text{MAC}_k(M)$ 
  if ( $|M| \neq \ell$ ) return  $\perp$ 
   $r \leftarrow_R \{0, 1\}^\ell$ 
   $Tag \leftarrow F_k(r \oplus M)$ 
  Return  $(r, Tag)$ 
```

L'algoritmo di verifica funziona nel seguente modo

```
 $\text{Ver}_k(M, (r, Tag))$ 
  if ( $|M| \neq \ell$ ) return  $\perp$ 
   $T \leftarrow F_k(r \oplus M)$ 
  if ( $T == Tag$ ) return 1
  else return 0
```

Dimostrare che tale schema non e' sicuro.

2. Sia $E : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ un cifrario a blocchi sicuro e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0,1\}^{\ell t}$ ($t \geq 2$). L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
  if ( $|M| \bmod \ell \neq 0 \vee |M| == 0$ ) return  $\perp$ 
  Sia  $M = M_1 || \dots || M_s \text{ // } |M_i| = \ell, e \parallel \text{indica concatenazione}$ 
   $IV \leftarrow_R \{0,1\}^\ell$ 
   $c_1 \leftarrow E_k(IV) \oplus M_1$ 
  for  $i = 2, \dots, s$ 
     $c_i \leftarrow E_k(M_i \oplus c_{i-1} \oplus M_{i-1})$ 
  end for
   $c \leftarrow c_1 || \dots || c_s$ 
  return  $(IV, c)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(IV, c)
  if ( $|c| \bmod \ell \neq 0 \vee |c| == 0$ ) return  $\perp$ 
  Sia  $c = c_1 || \dots || c_s$ 
   $M_1 \leftarrow E_k^{-1}(IV) \oplus c_1$ 
  for  $i = 2, \dots, s$ 
     $M_i \leftarrow E_k^{-1}(c_i) \oplus M_{i-1} \oplus c_{i-1}$ 
  end for
   $M \leftarrow M_1 || \dots || M_s$ 
  return  $M$ 
```

Dimostrare che tale cifrario non è sicuro contro attacchi a critttesto scelto.

$$M = \{0,1\}^{t\ell} \quad (t \geq 2)$$

$$\text{CONSIDERO } m_0 = 0^\ell || 0^\ell$$

$$c_1 \leftarrow E_k(IV) \oplus 0^\ell$$

$$c_2 \leftarrow E_k(0^\ell \oplus E_k(IV) \oplus 0^\ell \oplus 0^\ell)$$

$$c \leftarrow c_1 || c_2 = E_k(IV) || E_k(E_k(IV))$$

$$\text{return } (IV, c)$$

$$\text{CONSIDERO } m_1 = 1^\ell || 0^\ell$$

$$c_1 \leftarrow E_k(IV) \oplus 1^\ell$$

$$c_2 \leftarrow E_k(1^\ell \oplus E_k(IV) \oplus 1^\ell \oplus 0^\ell)$$

$$c \leftarrow c_1 || c_2 = E_k(IV) \oplus 1^\ell || E_k(E_k(IV))$$

$$c'_1 = c_1 \oplus 1^\ell$$

$$D_k(IV, c'_1 || c_2)$$

$A(Se)$:

$$m_0 = 0^{\ell} \| 0^{\ell}$$

$$m_1 = 1^{\ell} \| 0^{\ell}$$

$$(IV, C) = O_{ENC}(m_0, m_1) // C = C_1 \| C_2$$

$$C'_1 = C_1 \oplus 1^{\ell}$$

$$m = O_{DEC}(IV, C'_1 \| C_2)$$

if ($m == m_1$) return 1

else return 0

$$\Pr [ESP^{ind\text{-}CCA-1}(A) = 1] = 1$$

$$\Pr [ESP^{ind\text{-}CCA-0}(A) = 1] = 0$$

$$Adv^{ind\text{-}CCA}(A) = 1 - 0 = 1$$

4. In classe abbiamo studiato il paradigma PRF-as-a-MAC. Si consideri la seguente variante (randomizzata) del metodo. Sia $F : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente schema MAC $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza ℓ .

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```
MACk(M)
  if ( $|M| \neq \ell$ ) return  $\perp$ 
   $r \leftarrow_R \{0,1\}^\ell$ 
   $Tag \leftarrow F_k(r \oplus M)$ 
  Return  $(r, Tag)$ 
```

L'algoritmo di verifica funziona nel seguente modo

```
Verk(M, (r, Tag))
  if ( $|M| \neq \ell$ ) return  $\perp$ 
   $T \leftarrow F_k(r \oplus M)$ 
  if ( $T == Tag$ ) return 1
  else return 0
```

Dimostrare che tale schema non è sicuro.

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

$$r' = r \oplus M \oplus M'$$

$$Tag = F_k(r \oplus M) = F_k(r' \oplus M')$$

A(MA):

$$m_0 \leftarrow \{0,1\}^\ell$$

$$m_1 \leftarrow \{0,1\}^\ell$$

$$(r, Tag) = \text{Omac}(m_0)$$

$$\text{VF}(m_1, (r \oplus m_0 \oplus m_1, Tag))$$

Corso di Crittografia

Prova in Itinere del 09 Gennaio 2009

1. Definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a crittotesto scelto) per cifrari simmetrici.
2. Sia $E : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ un cifrario a blocchi sicuro e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0, 1\}^{t\ell}$ ($t \geq 1$). L'algoritmo di generazione della chiave si limita a restituire una stringa random di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enck(M)
  if ( $|M| \bmod \ell \neq 0 \vee |M| == 0$ ) return  $\perp$ 
  Sia  $M = m_1 \parallel \dots \parallel m_s$  //  $|m_i| = \ell$  e  $\parallel$  indica concatenazione
   $r_0 \leftarrow_R \{0, 1\}^\ell$ 
  for  $i = 1, \dots, s$ 
     $r_i \leftarrow E_k(r_{i-1})$ 
     $c_i \leftarrow m_i \oplus r_i$ 
  end for
   $c \leftarrow c_1 \parallel \dots \parallel c_s$ 
  return  $(r_0, c)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck( $r_0, c$ )
  if ( $|c| \bmod \ell \neq 0 \vee |c| == 0$ ) return  $\perp$ 
  Sia  $c = c_1 \parallel \dots \parallel c_s$ 
  for  $i = 1, \dots, s$ 
     $r_i \leftarrow E_k(r_{i-1})$ 
     $m_i \leftarrow c_i \oplus r_i$ 
  end for
   $M \leftarrow m_1 \parallel \dots \parallel m_s$ 
  return  $M$ 
```

Dimostrare che tale cifrario non è sicuro contro attacchi a crittotesto scelto.

$M = \{0,1\}^{t\ell}$, $t \geq 1$ Si consideri $m_0 = x, x \in \{0,1\}^\ell$ PER CUI SI HA

$$\text{Enc}_K(m_0) = E_K(r_0) \oplus x$$

CONSIDERO $m_0 = 0^\ell$ e $m_1 = 1^\ell$

$$\text{Enc}_K(m_0) = (r_0, E_K(r_0) \oplus 0^\ell = E_K(r_0))$$

$$\text{Enc}_K(m_1) = (r_0, E_K(r_0) \oplus 1^\ell)$$

$$\text{Dec}_K(r_0, E_K(r_0) \oplus 1^\ell) = m_1$$

$$\text{Dec}_K(r_0, E_K(r_0) \oplus 1^\ell \oplus 1^\ell) = m_0$$

A(SE):

$$m_0 = 0^\ell$$

$$m_1 = 1^\ell$$

$$(r', c') = \text{O}_{\text{ENC}}(m_1, m_2)$$

$$m = \text{O}_{\text{DEC}}(r', c' \oplus 1^\ell)$$

if ($m == m_0$) return 1

else return 0

$$\Pr [E_{\text{SP}_{\text{SE}}}^{\text{ind-cca-1}}(A) = 1] = 1$$

$$\Pr [E_{\text{SP}_{\text{SE}}}^{\text{ind-cca-0}}(A) = 1] = 0$$

$$\text{Adv}_{\text{SE}}^{\text{ind-cca}}(A) = 1$$

3. Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

```

Esp $H$ SPR-kk( $A$ )
 $k \leftarrow_R \mathcal{K}$ ;  $x_1 \leftarrow D$  //  $x_1$  è scelto secondo una distribuzione di probabilità arbitraria
 $x_2 \leftarrow A(k, x_1)$ ;
if ( $H_k(x_1) = H_k(x_2)$  and  $(x_1, x_2 \in D)$  and  $(x_1 \neq x_2)$ 
    Return 1
else Return 0

```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{SPR-kk}} = \Pr \left[\mathbf{Esp}_H^{\text{SPR-kk}}(A) = 1 \right]$$

Diciamo che H è una funzione Second Pre-image Resistant se tale vantaggio è prossimo a zero per ogni avversario polinomialmente limitato.

- (a) Si fornisca la definizione di funzione hash resistente alle collisioni (cr2).
 - (b) Si dimostri che ogni funzione resistente alle collisioni è anche una funzione Second Pre-image Resistant.
4. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per message authentication codes.
5. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ una funzione pseudocasuale sicura e si consideri il seguente schema MAC, $\Pi = (\mathbf{KeyGen}, \mathbf{MAC}, \mathbf{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $2\ell - 2$.

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo **MAC** è definito come segue:

```

MAC $k$ ( $M$ )
    if ( $|M| \neq (2\ell - 2)$ ) return  $\perp$ 
    Sia  $M = M[0]||M[1]$  //  $|M[i]| = \ell - 1$ 
     $Tag \leftarrow F_k(0||M[0])||F_k(1||M[1])$ 
    Return  $Tag$ 

```

E' questo metodo sicuro? Giustificare formalmente la risposta fornita.

m°3

(a) SIA $H: K \times D \rightarrow R$ UNA FUNZIONE HASH E SIA
A UN AVVERSARIO CHE HA ACCESSO A TALE FUNZIONE.
SI CONSIDERI IL SEGUENTE ESPERIMENTO:

$\text{ESP}_H^{\text{enc-uu}}(A)$:

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

$(x_1, x_2) \leftarrow A(K)$

$\text{if } (H_K(x_1) = H_K(x_2) \wedge x_1 \neq x_2 \wedge x_1, x_2 \in D) :$

return 1

else

return 0

L'AVVERSARIO A ENTRA SUBITO A CONOSCENZA DELLA CHIAVE UTILIZZATA DA H , QUINDI GENERA x_1 e x_2 . SE ACCADE CHE $H_K(x_1) = H_K(x_2)$, $x_1 \neq x_2$ e $x_1, x_2 \in D$, ALLORA È AVVENUTA UNA COLLISIONE.

IL VANTAGGIO DEGLI AVVERSARI È DEFINITO COME SEGUO:

$$\text{Adv}_H^{\text{enc-uu}}(A) = P_H[\text{ESP}_H^{\text{enc-uu}}(A) = 1]$$

DIREMO CHE H È UNA FUNZIONE HASH RESISTENTE ALLE COLLISIONI SE $\text{Adv}_H^{\text{enc-uu}}(A) \approx 0 \quad \forall A \text{ p.l.}$

(b) H_p : H È UNA FUNZIONE HASH RESISTENTE ALLE COLLISIONI

T_S : H È UNA FUNZIONE PRE-IMAGE RESISTANT

SUPPONIAMO PER ASSURDO CHE H NON SIA UNA FUNZIONE PRE-IMAGE RESISTANT, ALLORA ESISTE UN AVVERSARIO B SPR-KN IL CUI VANTAGGIO È MOLTO MAGGIORRE DI \emptyset , $\text{Adv}_H^{\text{SPR-KN}}(B) \gg 0$. SIA A UN AVVERSARIO CONTRO LA RESISTENZA ALLE COLLISIONI, CHE SFRUTTA B PER CONTRADDIRE L'IPOTESI.

$A(K)$:

$$x_1 \xleftarrow{R} D;$$

$$x_2 \xleftarrow{R} B(K, x_1);$$

if ($H_K(x_1) = H_K(x_2)$) return (x_1, x_2)

else

$$(x_1, x_2) \xleftarrow{R} D$$

return (x_1, x_2)

IN QUESTO CASO OTTENIAMO CHE IL VANTAGGIO DELL'AVVERSARIO A È:

$$\text{Adv}_H^{\text{CR2-KN}}(A) \geq \text{Adv}_H^{\text{SPR-KN}}(B) \gg 0$$

IL RISULTATO TROVATO CONTRADDICE L'IPOTESI INIZIALE E QUINDI OTTENIAMO UN ASSURDO.

Ogni funzione CR2-KN È ANCHE SPR-KN.

m° 5

SIA $M = \{0, 1\}^{2l-2}$ LA SPAZIO DEI MESSAGGI.

SIA $m_0 = X || X$ CON $X \in \{0, 1\}^{l-1}$

$\text{Tag}_0 = F_K(0 || X) || F_K(1 || X)$

SIA $m_1 = Y || Y$ CON $Y \in \{0, 1\}^{l-1}$

$\text{Tag}_1 = F_K(0 || Y) || F_K(1 || Y)$

A QUESTO PUNTO POSSO CONSIDERARE:

$m_2 = X || Y$

$\text{Tag}_2 = \text{Tag}_0[0] || \text{Tag}_1[1] = F_K(0 || X) || F_K(1 || Y)$

DEFINIAMO L'AVVERSARIO FORMALMENTE:

$A(\Pi)$:

$X, Y \in \{0, 1\}^{l-1} // X \neq Y$

$m_0 = X || X$

$\text{Tag}_0 = O_{MAC}(m_0)$

$m_1 = Y || Y$

$\text{Tag}_1 = O_{MAC}(m_1)$

$m_2 = X || Y$

$\text{Tag}_2 = \text{Tag}_0[0] || \text{Tag}_1[1]$

$\nabla F(m_2, \text{Tag}_2)$

$\Pr[\text{ESP}_{\Pi}^{\text{inf}-\text{Cma}}(A) = 1] = 1$

$\text{Adv}_{\Pi}^{\text{inf}-\text{Cma}}(A) = 1$

Corso di Crittografia

Prova in Itinere del 17 Gennaio 2007

1 Indistinguibilità

Introdurre e definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a messaggio scelto) per cifrari simmetrici.

2 Cifrari simmetrici

Si consideri la seguente variante del cifrario CBC\$ (che potremmo chiamare CBC1).

```
Enck(M)
  if (|M| mod n ≠ 0) ∨ (|M| = 0) return ⊥
  Sia M = M[1] … M[m]    // (|M[i]| = n)
  C[0] ← 1n    // 1n denota la stringa costituita da n bit tutti uguali a 1.
  for i = 1 to m do
    C[i] = Ek(C[i - 1] ⊕ M[i])
    // Ek è un cifrario a blocchi generico (ad es. AES).
  C ← C[1] … C[m]
  return C
```

Il vantaggio di tale cifrario, rispetto a CBC\$, è che, qui, la taglia del crittotesto prodotto è |M| bit, (CBC\$ produce crittotesti di taglia |M| + n).

Dimostrare formalmente che CBC1 non è un cifrario sicuro.

3 Funzioni Hash

In classe abbiamo definito il concetto di funzione resistente alle collisioni (**cr2 – kk**) nel seguente modo.

Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

```
Esperimento EspHcr2–kk(A)
  k ←R K;
  (x1, x2) ← A(k);
  if (Hk(x1) = Hk(x2)) and (x1 ≠ x2) and (x1, x2 ∈ D) Return 1
  else Return 0
```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{cr2-kk}} = \Pr [\mathbf{Esp}_H^{\text{cr2-kk}}(A) = 1]$$

Diciamo che H è una funzione resistente alle collisioni se tale vantaggio è piccolo per ogni avversario polinomialmente limitato.

Introduciamo adesso la nozione di funzione *division intractable*. Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

```

Esperimento  $\mathbf{Esp}_H^{\text{di-kk}}(A)$ 
   $k \leftarrow_R \mathcal{K};$ 
   $(x_1, \dots, x_n, y) \leftarrow A(k);$ 
  if ( $H_k(y)$  divide  $\prod_{i=1}^n H_k(x_i)$ ) and ( $y, x_1, \dots, x_n \in D$ ) and
    ( $n \geq 1$ ) and ( $\forall i = 1, \dots, n \ y \neq x_i$ )
      Return 1
    else Return 0

```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{di-kk}} = \Pr [\mathbf{Esp}_H^{\text{di-kk}}(A) = 1]$$

Diciamo che H è una funzione division intractable se tale vantaggio è piccolo per ogni avversario polinomialmente limitato.

Si dimostri che ogni funzione division intractable è anche una funzione resistente alle collisioni.

4 MAC

In classe abbiamo visto che un Message Authentication Code Π è, in generale, costituito da tre algoritmi, (KeyGen , MAC , VF) (l'algoritmo di generazione della chiave, l'algoritmo di generazione dell'autentica e l'algoritmo di verifica, rispettivamente). Inoltre abbiamo osservato che, a differenza dei cifrari, è possibile costruire Message Authentication Codes deterministici e sicuri. Descrivere il funzionamento (dapprima informalmente e poi presentando adeguato pseudocodice) dell'algoritmo di verifica nel caso in cui si considerino Message Authentication Codes deterministici.

5 Uso scorretto di RSA

Supponiamo che due fidanzati, Alice e Bob, decidano, romanticamente, di condividere lo stesso sistema RSA, nel seguente modo. Sia N un modulo RSA pubblico (la fattorizzazione di N è sconosciuta a tutti tranne che ad Alice e Bob), Alice utilizza come esponente pubblico e_1 e Bob utilizza come esponente pubblico e_2 . In particolare, supponiamo che $e_1 \neq e_2$ e $\gcd(e_1, e_2) = 1$. Se un terzo utente Oscar volesse mandare un messaggio m ad Alice, dapprima calcolerebbe $c_1 = m^{e_1} \bmod N$ e quindi

invierebbe (c_1, e_1) ad Alice (la presenza di e_1 sta ad indicare che, appunto, il messaggio è indirizzato ad Alice). Analogamente, volendo inviare m a Bob, dapprima Oscar calcolerebbe $c_2 = m^{e_2} \bmod N$ e quindi invierebbe (c_2, e_2) a Bob.

Purtroppo, tale approccio è del tutto insicuro. Supponiamo, che Oscar decida di inviare lo stesso messaggio m , cifrato come appena descritto, sia ad Alice che a Bob. Presentare un algoritmo che, a partire dai due crittotest (c_1, e_1) , (c_2, e_2) inviati da Oscar (che, ricordiamo, cifrano entrambi m), calcoli m in tempo polinomiale e senza conoscere la fattorizzazione di N .

Suggerimento: sfruttare il fatto che il massimo comune divisore (\gcd) di e_1 , e_2 è 1.

M°2

SIA $m \in \{0,1\}^{t_m}$ LO SPAZIO DEI MESSAGGI.

SI CONSIDERI $m_0 = X||X$ CON $X \in \{0,1\}^m$ ALLORA:

$$m = X||X$$

$$c[0] = 1^m$$

$$c[1] = E_k(c[0] \oplus X) = E_k(1^m \oplus X)$$

$$c[2] = E_k(E_k(1^m \oplus X) \oplus X)$$

SE $X = 0^m$ SI HA:

$$m_0 = 0^m || 0^m$$

$$c[0] = 1^m$$

$$c[1] = E_k(1^m)$$

$$c[2] = E_k(E_k(1^m))$$

SE $m_1 = X||Y$ SI HA:

$$c[0] = 1^m$$

$$c[1] = E_k(c[0] \oplus X) = E_k(1^m \oplus X)$$

$$c[2] = E_k(E_k(1^m \oplus X) \oplus Y)$$

DEFINISCO FORMALMENTE L'AVVERSARIO:

A(CBC1):

$$X, Y \in \{0,1\}^m$$

$$m_0 = X||X$$

$$m_1 = X||Y$$

$$C_0 = O_{ENC}(m_0, m_1)$$

$$C_1 = O_{ENC}(m_1, m_1)$$

if ($C_0 == C_1$) return 1

else return 0

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

$$\Pr[\text{Esp}^{\text{ind-CPA-0}}(A) = 1] = 0$$

$$\text{Adv}^{\text{ind-CPA}}(A) = 1 - 0 = 1$$

m° 3

H_p: H È UNA FUNZIONE DIVISION INTRACTABLE

T_S: H È UNA FUNZIONE RESISTENTE ALLE COLLISIONI

SUPPONIAMO PER ASSURDO CHE H NON È UNA FUNZIONE
RESISTENTE ALLE COLLISIONI, ALLORA ESISTE UN AVVERSARIO
B CR2-nn CON $\text{Adv}^{\text{CR2}-\text{nn}}(B) \gg 0$. SIA A UN AVVERSARIO
di-nn CHE SFUOTTA B PER CONTRADDIRE L'IPOTESI.

A(k):

$$(x_1, x_2) \leftarrow B(k);$$

$$y \leftarrow x_2;$$

if ($H_n(y) \neq H_n(x_1)$) return (x_2, y)

else:

$$(x_1, y) \leftarrow D$$

return (x_1, y)

IN QUESTO CASO:

$$\text{Adv}^{\text{di-nn}}(A) \geq \text{Adv}^{\text{CR2-nn}}(B) \gg 0$$

QUESTO È UN ASSURDO, QUINDI SE H È UNA FUNZIONE
DIVISION INTRACTABLE, ALLORA È ANCHE RESISTENTE
ALLE COLLISIONI.

Corso di Crittografia

Prova in Itinere del 17 Gennaio 2008

1 Indistinguibilità

In classe abbiamo visto che la definizione di indistinguibilità può essere formulata in termini di un solo esperimento nel seguente modo. Sia $(\text{KeyGen}, \text{Enc}, \text{Dec})$ un cifrario simmetrico e sia \mathcal{A} un algoritmo che ha accesso ad un oracolo che prende in input una coppia di stringhe (i due messaggi) e restituisce una stringa (un crittotesto). Consideriamo il seguente esperimento

```
Espind-cpa-cg( $\mathcal{A}$ )
   $b \leftarrow_R \{0, 1\}$ ;  $k \leftarrow_R K$       //  $K$  spazio delle chiavi
   $b' \leftarrow \mathcal{A}^{\text{Enc}(\text{LR}(\dots, b))}$ 
  If  $b = b'$  return 1 else return 0
```

Per tale esperimento definiamo il vantaggio dell'avversario

$$\text{Adv}^{\text{ind-cpa}}(\mathcal{A}) = 2 \cdot \Pr[\text{Esp}^{\text{ind-cpa-cg}}(\mathcal{A}) = 1] - 1$$

1. Si ri-definisca (formalmente) il concetto di indistinguibilità polinomiale, relativamente ad attacchi a messaggio scelto, utilizzando due esperimenti.
2. Si dimostri che le due definizioni sono equivalenti.

2 Cifrari simmetrici

Si consideri il seguente cifrario

```
Enck( $M$ )
  if ( $|M| \bmod n \neq 0$ )  $\vee$  ( $|M| = 0$ ) return  $\perp$ 
  Sia  $M = M[1] \cdots M[m]$       // ( $|M[i]| = n$ )
   $C[0] \leftarrow_R \{0, 1\}^n$ 
  for  $i = 1$  to  $m$  do
     $C[i] = E_k(C[i - 1]) \oplus M[i]$ 
    //  $E_k$  è un cifrario a blocchi generico (ad es. AES).
   $C \leftarrow C[1] \dots C[m]$ 
  return  $(C[0], C)$ 
```

Si dimostri che tale cifrario non è sicuro contro attacchi a crittotesto scelto.

$m^o \in$

SIA $M = \{0, 1\}^{t^m}$, $t \geq 1$, LO SPAZIO DEI MESSAGGI.

SI CONSIDERI $m_0 = 0^m$ ALLORA:

$$C[0] \leftarrow \{0, 1\}^m$$

$$C[1] = E_k(C[0]) \oplus 0^m = E_k(C[0])$$

return $(C[0], E_k(C[0]))$

SI CONSIDERI $m_1 = 1^m$ ALLORA:

$$C[0] \leftarrow \{0, 1\}^m$$

$$C[1] = E_k(C[0]) \oplus 1^m$$

return $(C[0], E_k(C[0]) \oplus 1^m)$

SE CONSIDERO:

$$\text{Dec}_k(C[0], E_k(C[0]) \oplus 1^m \oplus 1^m) = m_0$$

$$\text{Dec}_k(C[0], E_k(C[0]) \oplus 1^m) = m_1$$

DEFINISCO FORMALMENTE L'AVVERSARIO:

A(SE):

$$m_0 = 0^m$$

$$m_1 = 1^m$$

$$(C[0], C) \leftarrow O_{\text{ENC}}(m_0, m_1)$$

$$C' = C \oplus 1^m$$

$$m \leftarrow O_{\text{DEC}}(C[0], C')$$

if ($m == m_0$) return 1

else return 0

$$\Pr[\text{Esp}_{\text{SE}}^{\text{ind-cca-1}}(A) = 1] = 1$$

$$\Pr[\text{Esp}_{\text{SE}}^{\text{ind-cca-0}}(A) = 1] = 0$$

$$\text{Adv}_{\text{SE}}^{\text{ind-cca}}(A) = 1 - 0 = 1$$

3 Funzioni Hash

In classe abbiamo definito il concetto di funzione resistente alle collisioni (cr2-kk) nel seguente modo.

Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

```
Esperimento  $\text{Esp}_H^{\text{cr2-kk}}(A)$ 
   $k \leftarrow_R \mathcal{K};$ 
   $(x_1, x_2) \leftarrow A(k);$ 
  if  $(H_k(x_1) = H_k(x_2))$  and  $(x_1 \neq x_2)$  and  $(x_1, x_2 \in D)$  Return 1
  else Return 0
```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{cr2-kk}} = \Pr \left[\text{Esp}_H^{\text{cr2-kk}}(A) = 1 \right]$$

Diciamo che H è una funzione resistente alle collisioni se tale vantaggio è piccolo per ogni avversario polinomialmente limitato.

Introduciamo adesso la nozione di funzione *target collision resistant*. Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

```
Esperimento  $\text{Esp}_H^{\text{Tcr-kk}}(A)$ 
   $k \leftarrow_R \mathcal{K}; x_1 \leftarrow_R D$ 
   $x_2 \leftarrow A(k, x_1);$ 
  if  $(H_k(x_1) = H_k(x_2))$  and  $(x_1, x_2 \in D)$  and  $(x_1 \neq x_2)$ 
    Return 1
  else Return 0
```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{Tcr-kk}} = \Pr \left[\text{Esp}_H^{\text{Tcr-kk}}(A) = 1 \right]$$

Diciamo che H è una funzione Target collision resistant se tale vantaggio è piccolo per ogni avversario polinomialmente limitato.

Si dimostri che ogni funzione resistente alle collisioni è anche una funzione Target collision resistant.

4 MAC

Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per message authentication codes.

m°3

H_p: H È UNA FUNZIONE TARGET COLLISION RESISTANT

T_s: H È UNA FUNZIONE RESISTENTE ALLE COLLISIONI

SUPPONIAMO CHE H NON SIA UNA FUNZIONE RESISTENTE ALLE COLLISIONI, ALLORA ESISTE UN AVVERSARIO B CR2-HN TALE CHE $\text{Adv}_{\text{H}}^{\text{CR2-HN}}(\beta) \gg 0$. SIA A UN AVVERSARIO^{TER-HN} CHE SFRUTTA B PER CONTRADDIRE L'IPOTESI.

A(K, x₁):

(x₁', x₂') ← B(K)

if ($H_n(x_1) = H_n(x_1')$): return (x₁, x₂')

if ($H_n(x_2') = H_n(x_2)$): return (x₁', x₂')

else:

(x₁, x₂) ← D

return (x₁, x₂)

IL VANTAGGIO DI TALE AVVERSARIO RISULTA MAGGIORE O UGUALE AL VANTAGGIO DEGLI AVVERSARIO B, PER CUI SI HA:

$$\text{Adv}_{\text{H}}^{\text{TER-HN}}(A) \geq \text{Adv}_{\text{H}}^{\text{CR2-HN}}(\beta) \gg 0$$

QUESTO È UN ASSURDO, DATO CHE AVEVAMO IPOTIZZATO CHE H È UNA FUNZIONE TARGET COLLISION RESISTANT, PER CUI È ANCHE UNA FUNZIONE RESISTENTE ALLE COLLISIONI.

Corso di Crittografia

Prova in Itinere del 19 Dicembre 2014

1. Definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a crittotesto scelto) per cifrari simmetrici.
2. Sia $E : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ un cifrario a blocchi sicuro e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0,1\}^{2\ell}$. L'algoritmo di generazione della chiave si limita a restituire tre stringhe random (k, α, β) di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```

Enc(k,α,β)(M)
  if ( $|M| \neq 2\ell \vee |M| == 0$ ) return  $\perp$ 
  Sia  $M = M_1||M_2 // |M_i| = \ell$ , e  $||$  indica concatenazione
   $r \leftarrow_R \{0,1\}^\ell$ 
   $c_1 \leftarrow E_k(r \oplus \alpha) \oplus M_1$ ;  $c_2 \leftarrow E_k(r \oplus \beta) \oplus M_2$ 
   $c \leftarrow c_1||c_2$ 
  return  $(r, c)$ 

```

l'algoritmo di decifratura corrispondente è

```

Deck(r, c)
  if ( $|c| \neq 2\ell \vee |c| == 0$ ) return  $\perp$ 
  Sia  $c = c_1||c_2$ 
   $M_1 \leftarrow E_k(r \oplus \alpha) \oplus c_1$ ;  $M_2 \leftarrow E_k(r \oplus \beta) \oplus c_2$ 
   $M \leftarrow M_1||M_2$ 
  return  $M$ 

```

Dimostrare che tale cifrario non è sicuro in senso IND-CCA.

3. Definiamo il concetto di funzione XOR-collision resistant nel seguente modo. Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

Esperimento $\mathbf{Esp}_H^{\text{cr-XOR-kk}}(A)$

```

 $k \leftarrow_R \mathcal{K};$ 
 $(x_1, x_2, x_3) \leftarrow A(k);$ 
  if ( $H_k(x_1) = H_k(x_2 \oplus x_3)$ ) and ( $x_1 \neq (x_2 \oplus x_3)$ ) and ( $x_1, x_2, x_3 \in D$ ) Return 1
  else Return 0

```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{cr-XOR-kk}} = \Pr \left[\mathbf{Esp}_H^{\text{cr-XOR-kk}}(A) = 1 \right]$$

Diciamo che H è una funzione XOR-collision resistant se tale vantaggio è prossimo a zero per ogni avversario polinomialmente limitato.

- (a) Si definisca il concetto di funzione hash resistente alle collisioni (cr2 - kk).
 - (b) Si dimostri che ogni funzione resistente alle collisioni è anche una funzione XOR-collision resistant.
4. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per MAC.
5. Sia $F : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ una funzione pseudocasuale e si consideri il seguente schema MAC $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza 3ℓ .

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```

MAC $k$ ( $M$ )
  if ( $|M| \neq 3\ell$  or  $|M| = 0$ ) return  $\perp$ 
  Sia  $M = M[1]||M[2]||M[3]$  //  $|M[i]| = \ell$  e il simbolo  $||$  denota concatenazione
   $Tag \leftarrow (F_k(M[1]) \oplus F_k(M[3]))||(F_k(M[2]) \oplus F_k(M[3]))$ 
  Return  $Tag$ 

```

Dimostrare che tale schema non è sicuro.

$m^o 2$

SIA $M = \{0, 1\}^{2l}$ LO SPAZIO DEI MESSAGGI, PONIAMO $m = l$.

KeyGen return (K, α, β) DI LUNGHEZZA m .

SI CONSIDERI $m_0 = X || X$ CON $X \in \{0, 1\}^l$ ALLORA SI HA:
 $r \leftarrow \{0, 1\}^l$

$$c_1 \leftarrow E_K(r \oplus \alpha) \oplus X$$

$$c_2 \leftarrow E_K(r \oplus \beta) \oplus X$$

$$c \leftarrow c_1 || c_2 = E_K(r \oplus \alpha) \oplus X || E_K(r \oplus \beta) \oplus X$$

$$\text{return } (r, E_K(r \oplus \alpha) \oplus X || E_K(r \oplus \beta) \oplus X)$$

CONSIDERO $m_0 = 0^m || 0^m$ E $m_1 = 0^m || 1^m$ PER CUI SI HA:

$$Enc_{(K, \alpha, \beta)}(m_0) = (r_0, E_K(r_0 \oplus \alpha) || E_K(r_0 \oplus \beta))$$

$$Enc_{(K, \alpha, \beta)}(m_1) = (r_1, E_K(r_1 \oplus \alpha) || E_K(r_1 \oplus \beta) \oplus 1^m)$$

$$c_0 = c_1^0 || c_2^0 \quad \& \quad c_1 = c_1^1 || c_2^1$$

A QUESTO PUNTO DECIFRIAMO I DUE MESSAGGI COME SEGUI:

$$Dec_{(K, \alpha, \beta)}(r_0, c_1^0 || (c_2^0 \oplus 1^m)) = 0^m || 1^m = m_1$$

$$Dec_{(K, \alpha, \beta)}(r_1, c_1^1 || (c_2^1 \oplus 1^m)) = 0^m || 0^m = m_0$$

DA QUESTA OSSERVAZIONE POSSIAMO DETERMINARE

FORMALMENTE L'AVVERSARIO:

$A(\Sigma)$:

$$m_0 = 0^l || 0^l$$

$$m_1 = 0^l || 1^l$$

$$(r, c) \leftarrow O_{ENC}(m_0, m_1) // c = c_1 || c_2$$

$$m \leftarrow O_{DEC}(r, c_1 || (c_2 \oplus 1^m))$$

if ($m == m_0$) return 1
else return 0

$$\Pr[\text{Exp}_{\text{SE}}^{\text{ind-CCA-1}}(A) = 1] = 1$$

$$\text{Adv}_{\text{SE}}^{\text{ind-CCA}}(A) = 1 - 0 = 1$$

m°3

(a) SIA $H: K \times D \rightarrow R$ UNA FUNZIONE HASH E SIA A UN AVVERSARIO CR2-KK. SI CONSIDERI IL SEGUENTE ESPERIMENTO:

$\text{Esp}_H^{\text{CR2-KK}}(A)$:

$K \subseteq \mathbb{K}$;

$(x_1, x_2) \leftarrow A(K)$;

if ($H_K(x_1) = H_K(x_2) \wedge x_1 \neq x_2 \wedge x_1, x_2 \in D$):
return 1;

else:

return 0;

L'OBBIETTIVO DELL'AVVERSARIO È QUELLO DI RESTITUIRE x_1, x_2 , CONOSCENDO LA DESCRIZIONE DI H E LA CHIAVE K .

SE ACCADE CHE $H_K(x_1) = H_K(x_2)$, $x_1 \neq x_2$ E $x_1, x_2 \in D$, ALLORA A HA TROVATO UNA COLLISIONE. IL VANTAGGIO DI TALE AVVERSARIO È DEFINITO COME SEGUENTE:

$$\text{Adv}_H^{\text{CR2-KK}}(A) = \Pr[\text{Esp}_H^{\text{CR2-KK}}(A) = 1]$$

DICIAMO CHE H È UNA FUNZIONE RESISTENTE ALLE COLLISIONI (CR2-KK) SE $\text{Adv}_H^{\text{CR2-KK}}(A) \approx 0 \quad \forall A \text{ p.l.}$

m°3

(b) Hp: H È UNA FUNZIONE RESISTENTE ALLE COLLISIONI

TS: H È UNA FUNZIONE XOR-COLLISION RESISTANT

SUPPONIAMO CHE H NON SIA UNA FUNZIONE XOR-COLLISION RESISTANT, ALLORA ESISTE B CHE È UN AVVERSARIO CR-XOR-KN TACE CHE $\text{Adv}_H^{\text{cr}-\text{xor}-\text{kn}}(B) \gg 0$, ALLORA ESISTE A, CHE È UN AVVERSARIO CR2-KK, CHE SFROTTA B E CONTRADDICE L'IPOTESI.

A(κ):

$$(x_1, x_2, x_3) \leftarrow B(\kappa)$$

$$x_2 \leftarrow (x_2 \oplus x_3)$$

if ($H_\kappa(x_1) == H_\kappa(x_2)$): return (x_1, x_2)

else:

$$x_1, x_2 \leftarrow D$$

$$\text{return } (x_1, x_2)$$

IL VANTAGGIO DI A È IL SEGUENTE:

$$\text{Adv}_H^{\text{cr2-kn}}(A) \geq \text{Adv}_H^{\text{cr}-\text{xor}-\text{kn}}(B) \gg 0 \Rightarrow \text{ASSURDO!}$$

QUINDI L'IPOTESI INIZIALE È VERA E H È ANCHE UNA FUNZIONE XOR-COLLISION RESISTANT.

Corso di Crittografia

Prova in Itinere del 21 Dicembre 2015

1. Definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a crittotesto scelto) per cifrari simmetrici.
2. Sia $E : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ un cifrario a blocchi sicuro e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0,1\}^{2\ell}$. L'algoritmo di generazione della chiave si limita a restituire una stringa random k di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enc(k,α,β)(M)
  if ( $|M| \neq 2\ell \vee |M| == 0$ ) return  $\perp$ 
  Sia  $M = M_1||M_2$  //  $|M_i| = \ell$ ,  $e \parallel$  indica concatenazione
   $r \leftarrow_R \{0,1\}^\ell$ 
   $c_1 \leftarrow M_1 \oplus E_k(r)$ ;  $c_2 \leftarrow M_2 \oplus E_k(r)$ 
   $c \leftarrow c_1||c_2$ 
  return  $(r, c)$ 
```

l'algoritmo di decifratura corrispondente è

```
Deck(r, c)
  if ( $|c| \neq 2\ell \vee |c| == 0$ ) return  $\perp$ 
  Sia  $c = c_1||c_2$ 
   $M_1 \leftarrow E_k(r) \oplus c_1$ ;  $M_2 \leftarrow E_k(r) \oplus c_2$ 
   $M \leftarrow M_1||M_2$ 
  return  $M$ 
```

Dimostrare che tale cifrario non è sicuro in senso IND-CPA.

3. Definiamo il concetto di funzione ADD-collision resistant nel seguente modo. Sia $H : \mathcal{K} \times D \rightarrow R$ una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

```
Esperimento EspHcr-ADD-kk(A)
   $k \leftarrow_R \mathcal{K}$ ;
   $(x_1, x_2 \dots, x_{n+1}) \leftarrow A(k)$ ;
  if ( $H_k(x_{n+1}) = H_k(\sum_{i=1}^n x_i)$ ) and ( $x_1 \neq (\sum_{i=1}^n x_i)$ ) and ( $x_1, \sum_{i=1}^n x_i \in D$ )
    and ( $n \geq 1$ ) Return 1
  else Return 0
```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{cr-ADD-kk}} = \Pr \left[\mathbf{Esp}_H^{\text{cr-ADD-kk}}(A) = 1 \right]$$

Diciamo che H è una funzione ADD-collision resistant se tale vantaggio è prossimo a zero per ogni avversario polinomialmente limitato. Si dimostri che ogni funzione resistente alle collisioni è anche una funzione ADD-collision resistant.

4. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per MAC.
5. Sia $F : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ una funzione pseudocasuale, H una funzione hash resistente alle collisioni a valori in $\{0, 1\}^\ell$ e si consideri il seguente schema MAC, $\Pi = (\mathbf{KeyGen}, \mathbf{MAC}, \mathbf{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza $t\ell$, $t \geq 1$.

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo MAC è definito come segue:

```

MAC $k$ ( $M$ )
  if ( $|M| \bmod \ell \neq 0$  or  $|M| = 0$ ) return  $\perp$ 
   $\alpha = F_k(|M|)$ 
  Sia  $M = M[1]||...||M[t]$  //  $|M[i]| = \ell$  e il simbolo  $||$  denota concatenazione
   $Tag \leftarrow \oplus_{i=1}^t H(\alpha \oplus M[i])$ 
  Return  $Tag$ 

```

Dimostrare che tale schema non è sicuro.

$m^o 2$

SIA $M = \{0, 1\}^{2\ell}$, SI CONSIDERI $m = x \| x$ con $x \in \{0, 1\}^\ell$ ALLORA:
 $r \in \{0, 1\}^\ell$

$$C_1 \leftarrow x \oplus E_K(r)$$

$$C_2 \leftarrow x \oplus E_K(r)$$

$$C \leftarrow C_1 \| C_2 = x \oplus E_K(r) \| x \oplus E_K(r)$$

SIA $x = 0^\ell$ PER TACE VACORE SI HA:

$$C \leftarrow C_1 \| C_2 = E_K(r) \| E_K(r)$$

SIA $m_1 = 0^\ell \| 1^\ell$ PER TALI VALORI SI HA:

$$C \leftarrow C_1 \| C_2 = E_K(r) \| 1^\ell \oplus E_K(r)$$

$$\text{CON } m_0 = 0^\ell \| 0^\ell, C_1 \oplus C_2 = 0^\ell$$

$$\text{CON } m_1 = 0^\ell \| 1^\ell, C_1 \oplus C_2 = 1^\ell$$

DEFINIAMO FORMALMENTE L'AVVERSARIO:

A(SE):

$$m_0 = 0^\ell \| 0^\ell,$$

$$m_1 = 0^\ell \| 1^\ell,$$

$$(r, c) \leftarrow O_{\text{ENC}}(m_0, m_1); \| c = C_1 \| C_2$$

if $(C_1 \oplus C_2 = 1^\ell)$ return 1

else return 0

$$\Pr[\text{Esp}_{\text{SE}}^{\text{inc-CPA-1}}(A) = 1] = 1$$

$$\Pr[\text{Esp}_{\text{SE}}^{\text{ind-CPA-0}}(A) = 1] = 0$$

$$\text{Adv}_{\text{SE}}^{\text{ind-CPA}}(A) = 1 - 0 = 1$$

m° 3

H_p: H UNA FUNZIONE RESISTENTE ALLE COLLISIONI

Ts: H È UNA FUNZIONE ADD-COLLISION RESISTANT

SUPPONIAMO CHE H NON SIA UNA FUNZIONE ADD-COLLISION RESISTANT, ALLORA ESISTE B, CHE È UN AVVERSARIO CR-ADD-nK, TALE CHE $\text{Adv}^{CR\text{-ADD}-nK}(B) \gg 0$, ALLORA SIA A UN AVVERSARIO CR2-nK CHE SFUTTA B PER CONTRADDIRE L'IPOTESI.

A(n):

$(x_1, x_2, x_3) \leftarrow B(n); // n=2$

if ($x_3 \in D$ AND $x_3 \neq (x_1 + x_2)$
AND $H_n(x_3) = H_n(x_1 + x_2)$):

return $(x_3, x_1 + x_2)$

else:

$(x_1, x_2) \leftarrow D$

return (x_1, x_2)

OSS.

$$\sum_{i=1}^{m=2} x_i = x_1 + x_2$$

$$H_n(x_3) = H_n(\underbrace{x_1 + x_2})$$

$$x_1 \neq (x_1 + x_2)$$

$$x_1, (x_1 + x_2) \in D$$

EFFETTIVAMENTE NON SAPPIANO SE $x_3 \in D$ E SE $x_3 \neq (x_1 + x_2)$

IN QUESTO CASO IL VANTAGGIO DELL'AVVERSARIO È COSTI DEFINITO:

$$\text{Adv}^{CR2-nK}(A) \geq \text{Adv}^{CR\text{-ADD}-nK}(B) \Rightarrow \text{ASSURDO!}$$

m° 5

SIA $M = \{0,1\}^{\ell t}$, $t \geq 1$ LO SPAZIO DEI MESSAGGI, SI CONSIDERI $m_0 = X||Y$, CON $X, Y \in \{0,1\}^\ell$, PER TALE MESSAGGIO SI AVRÀ:

$$\text{MAC}_h(m_0) = \text{Tag} = H(2 \oplus X) \oplus H(2 \oplus Y)$$

A QUESTO PUNTO SE CONSIDERASSI $m_1 = Y||X$ IL TAG SARÀ:

$$\text{Tag}' = \text{Tag}$$

DEFINIAMO FORMALMENTE L'AVVERSARIO:

A(MA):

$$X, Y \leftarrow \{0,1\}^\ell // X \neq Y$$

$$\text{Tag} \leftarrow \text{Onac}(X||Y)$$

$$\text{Ovf}(Y||X, \text{Tag})$$

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

$$\text{Adv}^{\text{uf-cma}}(A) = 1$$

Corso di Crittografia

Prova in Itinere del 21 Dicembre 2020 – Gruppo A

1. Introdurre e definire formalmente il concetto di indistinguibilità (relativamente ad attacchi a crittotesto scelto) per cifrari simmetrici.
2. Sia $F : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ una funzione pseudocasuale e si consideri il seguente cifrario simmetrico. Lo spazio dei messaggi ammissibili è l'insieme $\{0, 1\}^{t\ell}$, $t \geq 1$. L'algoritmo di generazione della chiave si limita a restituire una stringa random k di lunghezza n . L'algoritmo di cifratura funziona nel seguente modo

```
Enc $k$ ( $M$ )  
    if ( $|M| \bmod \ell \neq 0$ ) return  $\perp$   
    Sia  $M = M_1 || \dots || M_t \quad |M_i| = \ell$ , e  $||$  indica concatenazione  
     $y_0 \leftarrow_R \{0, 1\}^\ell$   
    for  $i = 1, \dots, t$   
         $y_i \leftarrow F_k(y_0 \oplus \dots \oplus y_{i-1})$   
         $c_i \leftarrow y_i \oplus M_i$   
     $c \leftarrow c_1 || \dots || c_t$   
    return  $(y_0, c)$ 
```

l'algoritmo di decifratura corrispondente è

```
Dec $k$ ( $y_0, c$ )  
    if ( $|c| \bmod \ell \neq 0$ ) return  $\perp$   
    Sia  $c = c_1 || \dots || c_t$   
    for  $i = 1, \dots, t$   
         $y_i \leftarrow F_k(y_0 \oplus \dots \oplus y_{i-1})$   
         $M_i \leftarrow y_i \oplus c_i;$   
     $M \leftarrow M_1 || \dots || M_t$   
    return  $M$ 
```

Dimostrare che tale cifrario non è sicuro in senso IND-CCA.

3. In classe abbiamo definito il concetto di funzione resistente alle collisioni (**cr2 - kk**). Introduciamo adesso la nozione di funzione *double collision resistance*. Sia $H : \mathcal{K} \times D \rightarrow \{0, 1\}^t$, con $D \subset \{0, 1\}^*$ finito e non vuoto, una funzione hash e sia A un avversario che ha accesso ad essa. Si consideri il seguente esperimento

```

Esperimento  $\text{Esp}_H^{\text{double-cr-kk}}(A)$ 
   $k \leftarrow_R \mathcal{K};$ 
   $(y, x_1, x_2) \leftarrow A(k);$ 
  if ( $H_k(y \oplus H_k(x_1)) = H_k(y \oplus H_k(x_2))$  and  $(x_1 \neq x_2)$  and
       $(x_1, x_2 \in D, y \in \{0, 1\}^t)$  Return 1
  else Return 0

```

Il vantaggio di A è definito come

$$\mathbf{Adv}_H^{\text{double-cr-kk}} = \Pr \left[\text{Esp}_H^{\text{double-cr-kk}}(A) = 1 \right]$$

Diciamo che H è una funzione double-collision resistant se tale vantaggio è prossimo a zero per ogni avversario polinomialmente limitato.

Si dimostri che ogni funzione resistente alle collisioni è anche una funzione double-collision resistant.

4. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per message authentication codes.
5. Sia $F : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ una funzione pseudocasuale, si consideri il seguente schema MAC, $\Pi = (\text{KeyGen}, \text{MAC}, \text{Ver})$.

Lo spazio dei messaggi è definito come l'insieme delle stringhe di bit di lunghezza 3ℓ .

L'algoritmo di generazione della chiave si limita a restituire una stringa casuale di k bit. L'algoritmo **MAC** è definito come segue:

```

MAC $k$ ( $M$ )
  if ( $|M| \neq 3\ell$ ) return  $\perp$ 
   $r \leftarrow_r \{0, 1\}^\ell$ 
  Sia  $M = M[1]||M[2]||M[3]$  //  $|M[i]| = \ell$ 
   $Tag \leftarrow F_k(r \oplus M[1]) \oplus F_k(M[1] \oplus M[2] \oplus \overline{M[3]})$  //  $\overline{M}$  complementare di  $M$ 
  Return  $r, Tag$ 

```

L'algoritmo **Ver** è il seguente

```

Ver $k$ ( $M, (r, Tag)$ )
  if ( $|M| \neq 3\ell$ ) return  $\perp$ 
  Sia  $M = M[1]||M[2]||M[3]$  //  $|M[i]| = \ell$ 
   $y \leftarrow F_k(r \oplus M[1]) \oplus F_k(M[1] \oplus M[2] \oplus \overline{M[3]})$ 
  if ( $y = Tag$ ) Return 1 else return 0

```

Dimostrare che tale schema non e' sicuro.

m^o

SIA $M = \{0, 1\}^{t\ell}$, $t \geq 1$, LO SPAZIO DEI MESSAGGI E
 SIA $m_o = X || X$, CON $X \in \{0, 1\}^\ell$ ALLORA:

$$y_0 \leftarrow \{0, 1\}^\ell$$

$$y_1 = F_K(y_0 \oplus y_0)$$

$$c_1 = y_1 \oplus X$$

$$y_2 = F_K(y_1 \oplus y_1)$$

$$c_2 = y_2 \oplus X$$

$$C = C_1 || C_2$$

CONSIDERO $X = 0^\ell$:

$$C' = y_1 \oplus 0^\ell || y_2 \oplus 0^\ell$$

CONSIDERO $X = 0^\ell$ E $Y = 1^\ell$:

$$C'' = y_1 \oplus 0^\ell || y_2 \oplus 1^\ell$$

$$\text{Dec}(y_0, C'_1 || C'_2 \oplus 1^\ell) = m_1$$

$$\text{Dec}(y_0, C''_1 || C''_2 \oplus 1^\ell) = m_o$$

FORMALIZZIAMO L'AVVERSARIO:

A(SE):

$$m_o = 0^\ell || 0^\ell;$$

$$m_1 = 0^\ell || 1^\ell;$$

$$(y_0, C) = \text{OEnc}(m_o, m_1); || C = C_1 || C_2$$

$$m = \text{Odec}(y_0, C_1 || C_2 \oplus 1^\ell)$$

if ($m == m_o$) return 1

else return 0

$$\text{Adv}^{\text{ind-cca}}(A) = 1$$

m°3

H_p: H È UNA FUNZIONE RESISTENTE ACCE COLLISIONI

T_s: H È UNA FUNZIONE DOUBLE-COLLISION RESISTANT

SUPPONIAMO CHE H NON SIA UNA FUNZIONE DOUBLE
COLLISION RESISTANT, PER CUI ESISTE B, UN AVVERSARIO
DOUBLE-CR-UK CHE HA $\text{Adv}^{\text{D-CR-UK}}(B) \gg 0$, ACCORDA
ESISTE A CR2-UK CHE SFROTTA B E CONTRADDICE
L'IPOTESI.

A(κ):

$(y, x_1, x_2) \leftarrow B(\kappa);$

if ($H_\kappa(x_1) = H_\kappa(x_2)$): return (x_1, x_2) ;

else if ($H_\kappa(y \oplus H_\kappa(x_1)) = H_\kappa(y \oplus H_\kappa(x_2))$):

return $(y \oplus H_\kappa(x_1), y \oplus H_\kappa(x_2))$;

else:

$(x_1, x_2) \leftarrow D;$

return (x_1, x_2) ;

$\text{AdV}^{\text{CR2-UK}}(A) \geq \text{AdV}^{\text{double-CR-UK}}(B) \Rightarrow \text{ASSURDO!}$

m° 5

SIA $K = \{0, 1\}^{3l}$, si consideri $m_0 = X || X || X$, con $X \in \{0, 1\}^l$.

MAC_K(m₀):

$$n \leftarrow \{0, 1\}^l$$

$$m = X || X || X$$

$$\text{Tag} = F_K(n \oplus X) \oplus F_K(X \oplus X \oplus \bar{X})$$

return n, Tag

$$0^l || 0^l || 0^l$$

$$0^l || 1^l || 1^l$$

$$m_0 = 0^l || 0^l || 0^l$$

$$\text{Tag} = F_K(n) \oplus F_K(1^l)$$

$$m_1 = 0^l || 1^l || 1^l$$

$$\text{Tag} = F_K(n) \oplus F_K(1^l)$$

A(MA):

$$m_0 = 0^l || 0^l || 0^l;$$

$$(n, \text{tag}) \leftarrow \text{OnAC}(m_0)$$

$$m_1 = 0^l || 1^l || 1^l;$$

$$\text{OvF}(m_1, (n, \text{tag}))$$

$$\text{Adv}^{\text{uf-cma}}(A) = 1$$