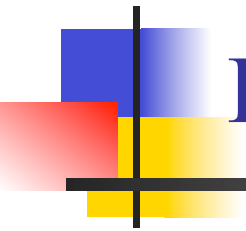
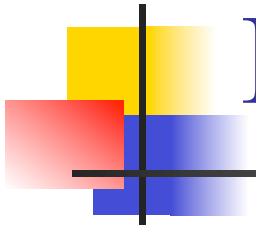


Corso di Crittografia

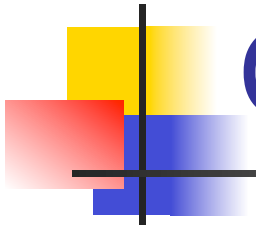
Prof. Dario Catalano

Cifrari Asimmetrici (Prima Parte)



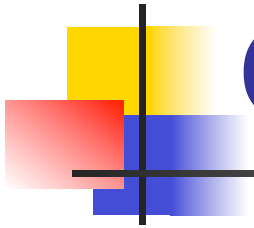
Introduzione

- Oggi parleremo di schemi di cifratura asimmetrici
  - Definizione di sicurezza.
  - Qualche esempio.
- Come i cifrari simmetrici, essi consisitono in
  - Un algoritmo di cifratura ENC
  - Un algoritmo di decifratura DEC
  - Un algoritmo di generazione della chiave KeyGen



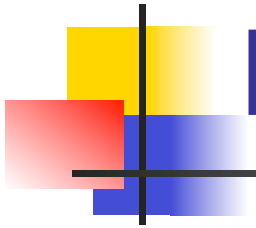
Cifrari Asimmetrici

- L'algoritmo KeyGen (randomizzato) restituisce una coppia (sk,pk)
- L'algoritmo Enc (randomizzato) prende in input a chiave pk e un messaggio m e restituisce un crittotesto C (o un simbolo speciale $\perp$)
- L'algoritmo Dec (deterministico) dall'input (sk,C) produce m (o il simbolo $\perp$).



Osservazioni

- L'algoritmo di generazione delle chiavi, e' in generale piu' complicato che nel caso simmetrico.
- Messaggi e crittotesti sono in generale elementi di gruppi finiti (non semplici stringhe)
  - Supporremo che esistono adeguati sistemi di codifica.
  - |m| indica la lunghezza della stringa binaria che codifica la rappresentazione di m.



Nozioni di sicurezza

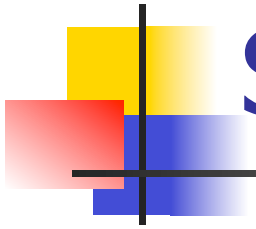
- L'avversario ha la possibilita' di cifrare senza bisogno di accedere all'oracolo.
- L'idea di base e' la stessa
  - L'avversario non deve essere in grado di trarre alcuna informazione non banale sul msg (a partire dal crittotesto).
- Anche nel caso asimmetrico distingueremo attacchi a msg scelto (cpa) o a crittotesto scelto (cca)

Definizione (ind-cpa)

- AE=(KeyGen, Enc, Dec) cifrario asimmetrico

$Esp_{AE}^{ind\text{-}cpa\text{-}1}(A)$	$Esp_{AE}^{ind\text{-}cpa\text{-}0}(A)$
$(pk,sk) \leftarrow_R KeyGen$	$(pk,sk) \leftarrow_R KeyGen$
$b \leftarrow A^{Enc_{pk}(LR(.,.,1))}$	$b \leftarrow A^{Enc_{pk}(LR(.,.,0))}$
Return b	Return b

$$Adv^{ind\text{-}cpa}(A)=|Pr[Esp_{AE}^{ind\text{-}cpa\text{-}1}(A)=1]-Pr[Esp_{AE}^{ind\text{-}cpa\text{-}0}(A)=1]|$$



Sicurezza contro attacchi attivi

- All'avversario e' data la possibilita' di accedere anche ad un oracolo di decifratura.
- Tale modello e' molto piu' rilevante che nel caso simmetrico.

Definizione (ind-cca)

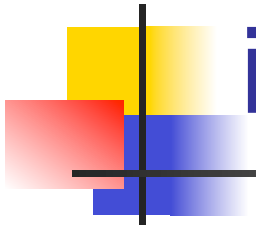
- AE=(KeyGen, Enc, Dec) cifrario simmetrico

$Esp_{SE}^{ind\text{-}cca\text{-}1}$ (A)	$Esp_{SE}^{ind\text{-}cca\text{-}0}$ (A)
$(pk,sk) \leftarrow_R$ KeyGen	$(pk,sk) \leftarrow_R$ KeyGen
$b \leftarrow A^{Enc_{pk}(LR(.,.,1)),Dec_{sk}(.)}$	$b \leftarrow A^{Enc_{pk}(LR(.,.,0)),Dec_{sk}(.)}$
If A imbroglia Return 0	If A imbroglia Return 0
else return b	else return b

$Adv^{ind\text{-}cca}(A)=|Pr[Esp_{AE}^{ind\text{-}cca\text{-}1}(A)=1] - Pr[Esp_{AE}^{ind\text{-}cca\text{-}0}(A)=1]|$

A imbroglia se interroga $D_k(.)$ su un crittotesto gia' restituito da $Enc_{pk}(LR(.,.,1))$

Perche' CCA e' un modello importante



- La definzione di sicurezza contro attacchi CCA e' abbastanza artificiale.
- La sua reale motivazione nasce da esigenze concrete.
- Molte applicazioni pratiche ci inducono a pensare che questa sia la definizione "giusta" da adottare.

Non malleabilità

Un cifrario sicuro in senso IND-CCA garantisce non malleabilità

- Sia AE=(KeyGen, Enc, Dec) sicuro in senso IND-CPA ($\mathcal{M}$ spazio dei messaggi)
- F: $\mathcal{M} \rightarrow \mathcal{M}$ funzione efficientemente computabile.
- Sia AE malleabile relativamente ad F

  Enc(F(m)) pubblicamente calcolabile dati Enc(m) ed F

  Esiste una procedura **MAUL**

  MAUL(Enc(m),F)→Enc(F(M))
- AE **non può essere sicuro** in senso IND-CCA

Non malleabilità (cont.)

A (AE,F)

$m_0, m_1 \leftarrow_R \mathcal{M}$;

$C \leftarrow O_{\mathcal{E}}(m_0, m_1)$;

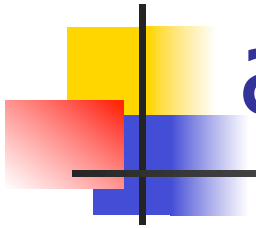
$C' \leftarrow$ **MAUL**(C, F)

$m \leftarrow O_{\mathcal{D}}(C')$

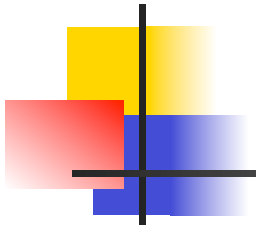
IF $(m == F(m_1))$ return 1

ELSE return 0

Quante domande di cifratura autorizziamo?

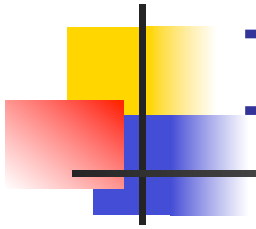


- L'avversario e' autorizzato a fare un qualunque numero (limitato) di encryption queries.
- In realta' il numero di domande non e' cosi' significativo nel caso asimmetrico.
- Se aumenta il num di domande il vantaggio aumenta in modo molto limitato.



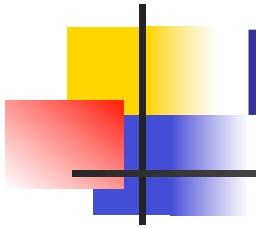
- AE=(KeyGen, Enc, Dec) cifrario simmetrico
- B avversario ind-cca che fa al piu' q_e domande (enc)
- Esiste A avversario ind-cca che fa al piu' 1 domanda (enc), che ha lo stesso tempo di calcolo di B e tale che

$$\mathrm{Adv}_{AE}^{\mathtt{ind-cca}}(B) \leq q_e \cdot \mathrm{Adv}_{AE}^{\mathtt{ind-cca}}(A)$$



Interpretazione qualitativa

- Un cifrario asimmetrico per il quale e' autorizzata una sola domanda (enc) e' altrettanto sicuro di un sistema nel quale autorizziamo tante domande.
  - Un risultato analogo vale per ind-cpa
  - La dimostrazione e' complicata
- Informalmente, la ragione che rende possibile tale risultato e' che l'avversario puo' cifrarsi da solo ogni messaggio che vuole.



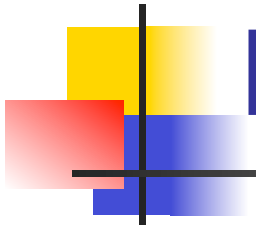
Hybrid Encryption

Costruire cifrari asimmetrici combinando tecniche simmetriche e asimmetriche

1. Cifrare (con un cifrario simmetrico) i dati usando una chiave k
2. Cifrare (con un cifrario asimmetrico) la chiave k

Vantaggi:

- Velocità
- Nessun problema di codifica.



Hybrid Encryption

AE=(KeyGen^{a}, Enc^{a}, Dec^{a}) cifrario asimmetrico

SE=(KeyGen^{s}, Enc^{s}, Dec^{s}) cifrario simmetrico

HE=(KeyGen^{H}, Enc^{H}, Dec^{H})

KeyGen^{H}=KeyGen^{a}

Hybrid Encryption

$\mathbf{Enc^H(pk,m)}$

$\mathbf{k \leftarrow_R KeyGen^s;}$

$\mathbf{C^s \leftarrow Enc^s(k,m);}$

$\mathbf{C^a \leftarrow Enc^a(pk,k);}$

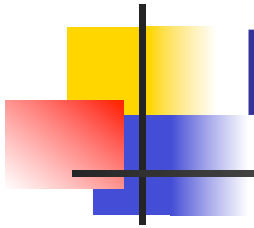
$\mathbf{return\ (C^s, C^a)}$

$\mathbf{Dec^H(sk, (C^s, C^a))}$

$\mathbf{k \leftarrow Dec^a(sk, C^a);}$

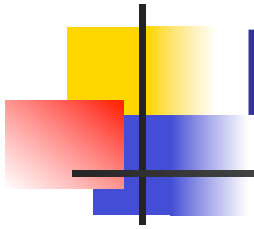
$\mathbf{m \leftarrow Dec^s(k, C^s);}$

$\mathbf{return\ m}$



Primi cifrari asimmetrici

- Inizialmente studieremo due cifrari sicuri solo relativamente ad attacchi i tipo cpa.
- Cifrario El Gamal (1984)
- Cifrario Paillier (1999)
  - Versione semplificata



El Gamal

KeyGen

$x \leftarrow_R \{1,..,q\}$; $h \leftarrow g^x$; $PK=(g,h,p,q)$; $SK=(x)$

Enc(PK,M)

$r \leftarrow_R \{1,..,q\}$; $C_1 \leftarrow g^r$; $C_2 \leftarrow h^r M$;

Dec(SK, C_1,C_2)

$A \leftarrow C_1^x$; $M \leftarrow C_2/A$

Il problema Diffie-Hellman Decisionale

G gruppo ciclico di ordine m, g generatore di G

$Esp_{G,g}^{ddh-1}$ (A)	$Esp_{G,g}^{ddh-0}$ (A)
$x,y \leftarrow_R Z_m$; $z \leftarrow xy \bmod m$	$x,y,z \leftarrow_R Z_m$;
$X \leftarrow g^x$; $Y \leftarrow g^y$; $Z \leftarrow g^z$;	$X \leftarrow g^x$; $Y \leftarrow g^y$; $Z \leftarrow g^z$;
$d \leftarrow_R A(X,Y,Z)$	$d \leftarrow_R A(X,Y,Z)$
Return d	Return d

$$Adv^{cdh}_{G,g}(A)=Pr[Esp^{ddh-1}_{G,g}(A)=1]-Pr[Esp^{ddh-0}_{G,g}(A)=1]$$