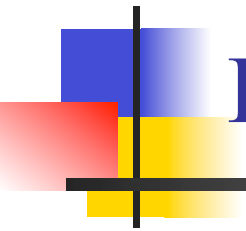
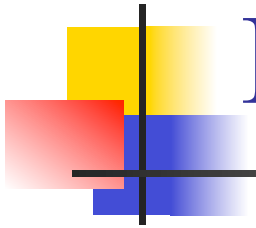


Corso di Crittografia

Prof. Dario Catalano

Funzioni e Permutazioni Pseudo-casuali: Introduzione



Introduzione

- Funzioni (PRF) e permutazioni (PRP) pseudo casuali sono tra le primitive piu' importanti della crittografia (specialmente simmetrica)
- Particolarmente utili per analizzare la sicurezza dei cifrari a blocchi (o meglio dei protocolli su questi basati)
- Oggi introdurremo tali oggetti e ne discuteremo le proprieta' di base.

Famiglie di funzioni

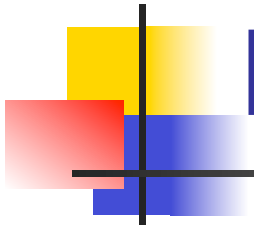
- *Mappa* del tipo

  $F: K \times D \rightarrow R$

  - Per noi K e' l'insieme delle chiavi, D il dominio e R il codominio.
  - Tutti insiemi finiti e non vuoti.
- Per semplicita' $F_K(X)=F(K,X)$
- F_K e' un'*istanza* di F
- Dunque, F definisce un'insieme (o famiglia) di funzioni.

Parametri e notazione

- $K = \{0,1\}^k$, k intero che stabilisce la lunghezza della chiave.
- $D = \{0,1\}^\ell$, ℓ intero che stabilisce la lunghezza dell'input.
- $R = \{0,1\}^L$, L intero che stabilisce la lughezza dell'output.
- $a \leftarrow_R A$, indica l'operazione di scelta casuale (distribuzione uniforme) di un elemento in A.



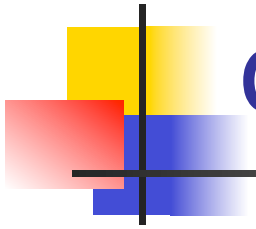
Permutazioni

- Una permutazione π e' una biezione nella quale D=R.
- Proprieta': per ogni x in D esiste un solo y in R tale che $\pi(x)=y$.

Esempi:

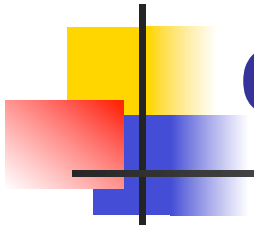
- DES e' una permutazione (k=56, ℓ=L=64)
- AES e' una permutazione (k=ℓ=L=128)

Funzioni e Permutazioni casuali - I



- Consideriamo le famiglie:
  - Func(D,R), famiglia di TUTTE le funzioni da D a R.
    - Denotata anche Func(ℓ,L).
  - Perm(D), famiglia di TUTTE le permutazioni su D.
    - Denotata anche Perm(ℓ)

Funzioni e Permutazioni casuali - II



- Una istanza (casuale) di Func(D,R) e' dunque una funzione casuale da D a R
- Una istanza (casuale) di Perm(D) e' dunque una permutazione casuale su D.
- Oggi studieremo questi strani oggetti.

Funzioni casuali

- F(D,R) famiglia di tutte le funzioni da D a R.
- La chiave (che descrive ogni istanza) e' la mera descrizione della funzione

Esempio:

- Ordiniamo gli input X_1, X_2, X_3,...
- La chiave per una (specifica) funzione f e' la lista $f(X_1)$, $f(X_2)$, $f(X_3)$,...

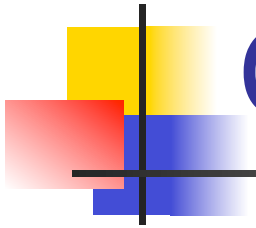
Esempio - I

- Func(4,2) (ℓ=4,L=2).
- D=$\{0,1\}^4$, R=$\{0,1\}^2$.
- x in {0000,0001,0010,0011,0100,0101,0110,0111, 1000,1001,1010,1011,1100,1101,1110,1111}
- f(x) in {00,01, 10,11}
- A questo punto non ci resta che definire f()

Esempio - II

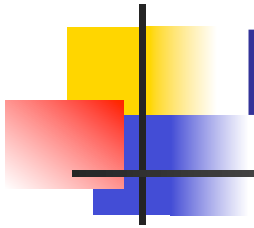
00 00	00 01	00 10	00 11	01 00	01 01	01 10	01 11	10 00	10 01	10 10	10 11	11 00	11 01	11 10	11 11
11	01	00	11	10	00	10	01	10	11	00	10	01	00	11	01

- Dunque la chiave e' (11,01,00,11,10,00,10,01,10,11,00,10,01,00,11,01)
- Lo spazio delle chiavi e' dato da tutte le possibili sequenze dello stesso tipo.
- $2^{2 \cdot 24} = 2^{2 \cdot 16} = 2^{32}$



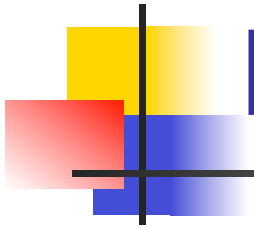
Osservazioni

- Si noti che a input uguali corrispondono sempre output uguali.
- Il termine “funzione casuale” e’ molto fuorviante
- La “casualita’ ” non e’ riferita alla funzione ma alla scelta della stessa.
- Implicitamente, non abbiamo fatto altro che scegliere una funzione a caso, tra le tante possibili.
- Fermiamoci un attimo per capire meglio questi strani oggetti.



Permutazioni Casuali

- Perm(D) contiene tutte le possibili permutazioni su D.
- La chiave che descrive una particolare istanza e' quindi una delle permutazioni in questione.
- Le perm casuali sono un po' piu' difficili da gestire (rispetto alle funzioni).



Funzioni Pseudo-casuali

- Famiglia di funzioni che “sembrano” casuali.
- Computazionalmente indistinguibili dalle funzioni casuali.
- Avendo accesso “a scatola chiusa” (o black box) alla funzione e’ difficile stabilire se si abbia di fronte una vera funzione casuale oppure una funzione pseudo casuale.
- Cerchiamo di arrivare ad una definizione ragionevole di questo concetto.

Definizione

- Sia F: K × D → R una famiglia di funzioni (pubblica)
- A avversario che ha accesso black box alla funzione in questione

Esp_F^{prf-1} (A)	Esp_F^{prf-0} (A)
$K \leftarrow_R K$	$g \leftarrow_R Func(D,R)$
$b \leftarrow A^{F_K}$	$b \leftarrow A^g$
Return b	Return b
//Funz. PC	//Funz Casuale

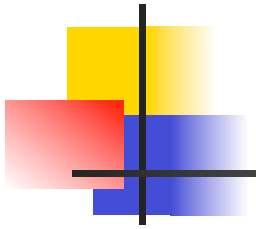
Definizione

- F: K × D → R, famiglia di funzioni (pubblica)

Esp_F^{prf-1} (A)	Esp_F^{prf-0} (A)
$K \leftarrow_R K$	$g \leftarrow_R Func(D,R)$
$b \leftarrow A^{F_K}$	$b \leftarrow A^g$
Return b	Return b
// Funz. PseudoCasuale	// Funz. Casuale

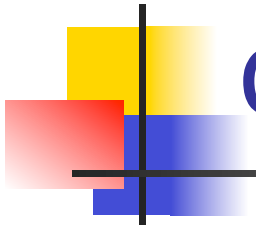
$$Adv(A)=|Pr[Esp_F^{prf-1}(A)=1] - Pr[Esp_F^{prf-0}(A)=1]|$$

- La prf e' sicura se tale vantaggio e' "piccolo"



- Si noti, (ancora una volta!) che la definizione non limita il comportamento dell'avversario
- Possiamo pero' limitare, il numero di domande che e' autorizzato a porre, il suo tempo di calcolo, la lunghezza totale delle domande.
- In pratica e' importante fare attenzione a questi dettagli.

Interpretazione della definizione

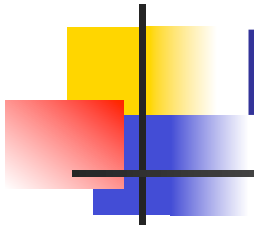


- La nostra definizione si limita ad associare (ad ogni) avversario un certo vantaggio.
- Che vuol dire allora che una prf F e' sicura?
- Intuitivamente, diciamo che F e' sicura se tale vantaggio rimane basso per tutti gli avversari che dispongono di risorse ragionevolmente limitate.

Ulteriori osservazioni

- Tutte (o quasi) le definizioni che vedremo avranno a che fare con esperimenti che coinvolgono un avversario A.
- Ci sara' sempre un vantaggio (associato ad A) che misura l'abilita' di A nel rompere il sistema.

Permutazioni Pseudo-casuali



- Molto simili alla gia' viste funzioni.
- In questo caso pero' possiamo immaginare due tipi diversi di domande da porre al nostro terminale.
  - L'avversario ha accesso black box ad una permutazione g (chosen message attack)
  - L'avversario ha accesso a g e g^{-1} (chosen ciphertext attack)

Definizione (cpa)

- Sia F: K × D → D una famiglia di permutazioni (pubblica)
- A avversario che ha accesso black box alla permutazione in questione

$Esp_F^{prp\text{-}cpa\text{-}1}$ (A)	$Esp_F^{prp\text{-}cpa\text{-}0}$ (A)
$K \leftarrow_R K$	$g \leftarrow_R Perm(D)$
$b \leftarrow A^{F_K}$	$b \leftarrow A^{g}$
Return b	Return b