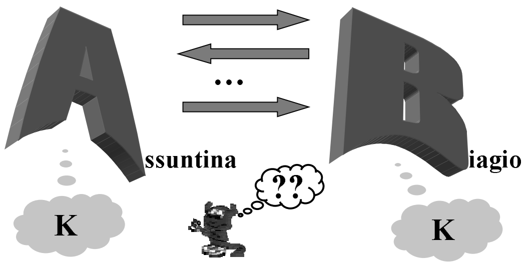
Accordo su una chiave



Diffie-Hellman 0

Diffie-Hellman [1976]

primo p, generatore g di Z_p^*

Diffie-Hellman 1

Generatori

g è generatore di Z_p^* se $\{g^i | 1 \le i \le p-1\} = Z_p^*$

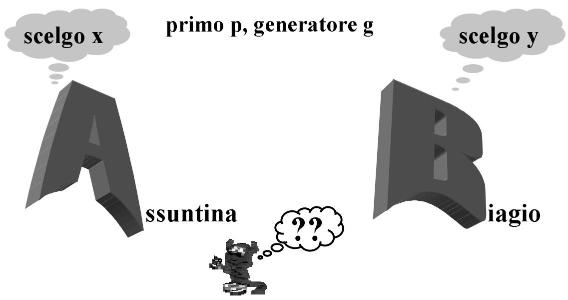
Esempio:

g = 2 è un generatore di Z_{11}^*

2^{10}	= 1024	= 1 mod 11
2^1		= 2 mod 11
2^8	= 256	= 3 mod 11
2^2		= 4 mod 11
2^4	= 16	= 5 mod 11
2^9	= 512	= 6 mod 11
2^7	= 128	= 7 mod 11
2^3		= 8 mod 11
2^6	= 64	= 9 mod 11
2^5	= 32	= 10 mod 11

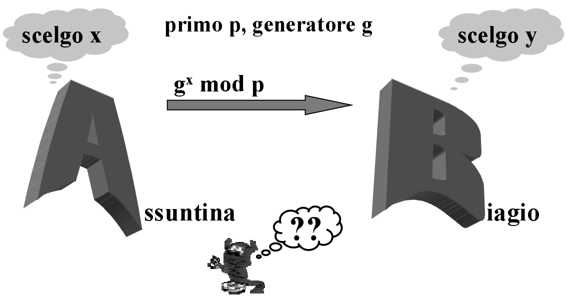
Diffie-Hellman 2

Diffie-Hellman [1976]



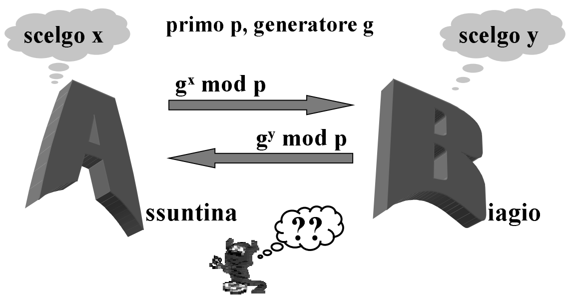
Diffie-Hellman 3

Diffie-Hellman [1976]



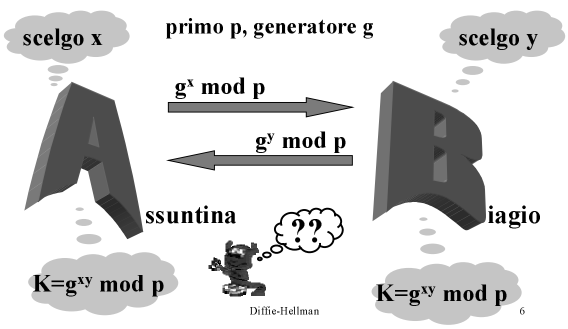
Diffie-Hellman 4

Diffie-Hellman [1976]

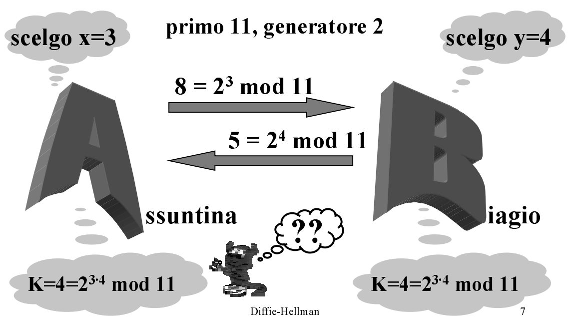


Diffie-Hellman 5

Diffie-Hellman [1976]



Diffie-Hellman: "piccolo" esempio



Logaritmo discreto

Dati a,n,b calcolare x tale che $a^x = b \mod n$

- Esempio: $3^x = 7 \mod 13$ soluzione $x = 6$
- Se n è primo, i migliori algoritmi hanno complessità

$$L_n[a,c] = O(e^{(c+o(1))(\ln n)^a(\ln\ln n)^{1-a}})$$

con $c > 0$ ed $0 < a < 1$

- **Miglior algoritmo: Number field sieve**

tempo medio euristico $L_n[1/3, 1.923]$

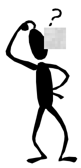
Logaritmo discreto

La sicurezza di molte tecniche crittografiche si basa sulla intrattabilità del logaritmo discreto:

- Crittosistema di El-Gamal
- Firme digitali di El-Gamal e DSS
- Accordo su chiavi di Diffie-Hellman
- …

Problema di Diffie-Hellman

Input: primo p, generatore g,
g^x mod p, g^y mod p
Calcolare: g^{xy} mod p



Il miglior algoritmo conosciuto calcola prima il logaritmo discreto $x \leftarrow \log_{g,p}(g^x \bmod p)$
… ma non si sa se sono equivalenti!

Generatori di Z_n^*

- Ordine di $\alpha \in Z_n^*$ = il più piccolo intero positivo r tale che $\alpha^r = 1 \mod n$
- α è generatore di Z_n^* se ha ordine $\phi(n)$
- Z_n^* ha un generatore $\Leftrightarrow$ $n = 2,4,p^k,2p^k$, con p primo e $k\geq 1$
  - In particolare, se p è primo, allora Z_p^* ha un generatore
- Se α è un generatore di Z_n^*, allora
  - $Z_n^* = \{\alpha^i \bmod n \mid 0 \leq i \leq \phi(n)-1\}$
  - $b = \alpha^i \bmod n$ è un generatore di Z_n^* $\Leftrightarrow$ $\gcd(i,\phi(n))=1$
  - il numero di generatori in Z_n^* è $\phi(\phi(n))$.

Scelta di un generatore

- p primo, $p - 1 = p_1^{e_1} p_2^{e_1} \dots p_k^{e_k}$
- α è un generatore di $Z_p^* \Leftrightarrow \begin{cases} \alpha^{(p-1)/p_1} \neq 1 \mod p \\ \dots \\ \alpha^{(p-1)/p_k} \neq 1 \mod p \end{cases}$

Diffie-Hellman 12

Scelta di un generatore

- p primo, $p - 1 = p_1^{e_1} p_2^{e_1} \dots p_k^{e_k}$
- α è un generatore di $Z_p^* \Leftrightarrow \begin{cases} \alpha^{(p-1)/p_1} \neq 1 \mod p \\ \dots \\ \alpha^{(p-1)/p_k} \neq 1 \mod p \end{cases}$

Scegli_generatore (p, $(p_1,e_1,p_2,e_2,\dots,p_k,e_k)$)
1. $\alpha \leftarrow$ elemento scelto a caso in Z_p^*
2. if ($\alpha^{(p-1)/p_1} \neq 1$ mod p **and** … **and** $\alpha^{(p-1)/p_k} \neq 1$ mod p)
then esci **trovato!**
else go to **1.**

Diffie-Hellman 13

Probabilità successo singola iterazione

- Numero di generatori modulo un primo p è

$$\phi(\phi(p)) = \phi(p-1)$$
$$> (p-1) / (6 \cdot \ln\ln(p-1))$$

per ogni intero $n \geq 5$, $\phi(n) > n/(6 \ln\ln n)$

- Probabilità che un elemento a caso in Z_p^* sia generatore

$$= \frac{\phi(\phi(p))}{\phi(p)} > \frac{p-1}{\phi(p)\, 6 \cdot \ln\ln(p-1)} = \frac{1}{6 \cdot \ln\ln(p-1)}$$

Diffie-Hellman 14

Analisi di Scegli_generatore

Numero medio di iterazioni $< 6 \cdot \ln\ln(p-1)$

512 bit	$6 \cdot \ln\ln(2^{512}) \approx 35{,}23$
1024 bit	$6 \cdot \ln\ln(2^{1024}) \approx 39{,}38$

Diffie-Hellman 15

Puzzle di Merkle

Puzzle la cui soluzione richiede t operazioni

Esempio:

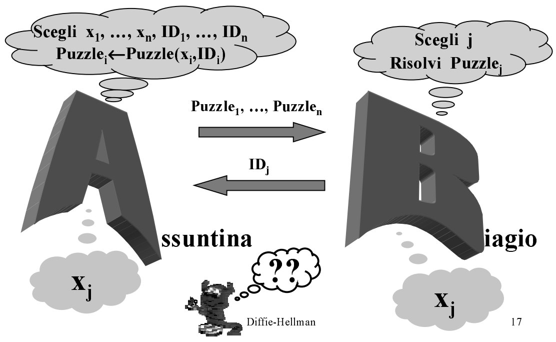
Puzzle (x,ID)
Scegli una chiave k
Computa $y \leftarrow$ CBC-DES$_k$(x,ID)
return (y, primi 20 bit di k)

Soluzione del puzzle: x

Richiede 2^{35} operazioni in media

Diffie-Hellman 16

Puzzle di Merkle



Diffie-Hellman 17

Puzzle di Merkle

- Computazioni di :
  - Costruzione di n puzzle tempo θ(n)
- Computazioni di :
  - Risoluzione di un puzzle tempo θ(t)
- Computazioni di :
  - Risoluzione di n/2 puzzle in media tempo θ(t·n)

Diffie-Hellman 18

Puzzle di Merkle

Se n = θ(t)

- Computazioni di :
  - Costruzione di n puzzle tempo θ(n)
- Computazioni di :
  - Risoluzione di un puzzle tempo θ(n)
- Computazioni di :
  - Risoluzione di n/2 puzzle in media tempo $\theta(n^2)$

Diffie-Hellman 19