Key Management

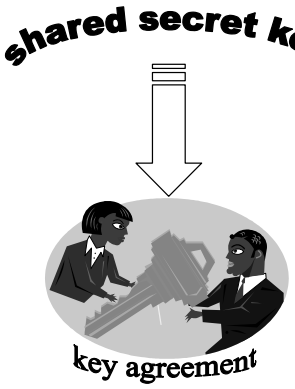
Accordo sulla chiave segreta

“uno a uno”

Incontro
Corriere

“molti a molti”

Internet



“modifica frequente”

Session key
One-time key

CON PRECEDENTE KA

Chiave in uso

- ***Master key***
- ***KDC***

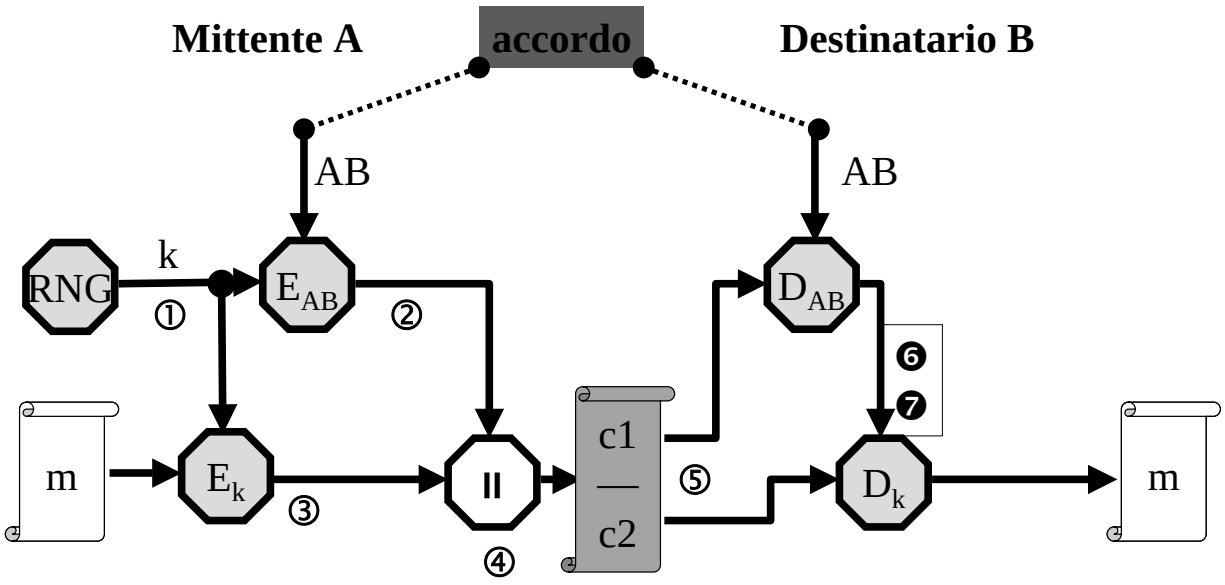
SENZA PRECEDENTE KA

- ***Scambio di Diffie-Hellman***
- ***Cifrario asimmetrico***

Key Management

- **Master key**

La master key



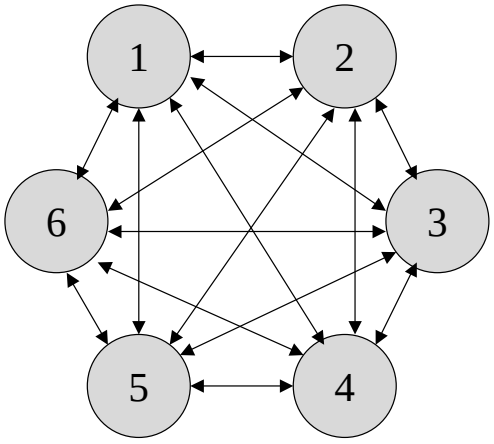
La chiave AB cifra solo le chiavi k e può avere una vita “lunga”
La chiave k cifra messaggi anche “lunghi” ed è usata una volta sola

Key Management

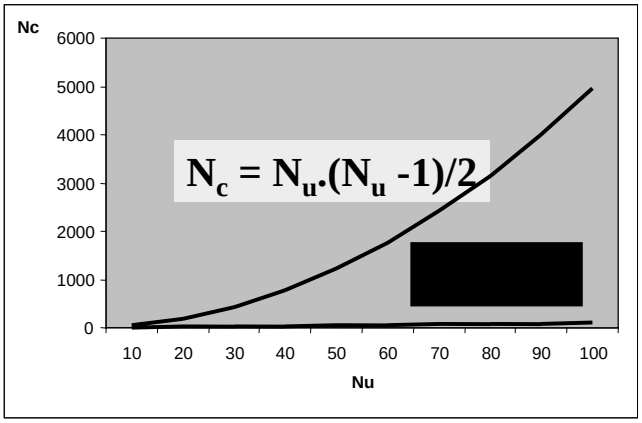
- **Key Distribution Center**

Numero di chiavi in circolazione

Comunità di utenti



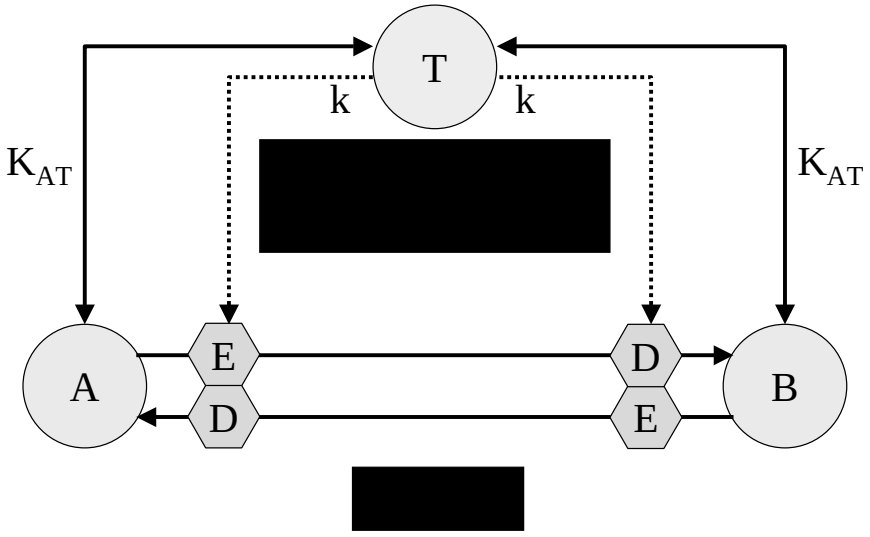
Non è scalabile!

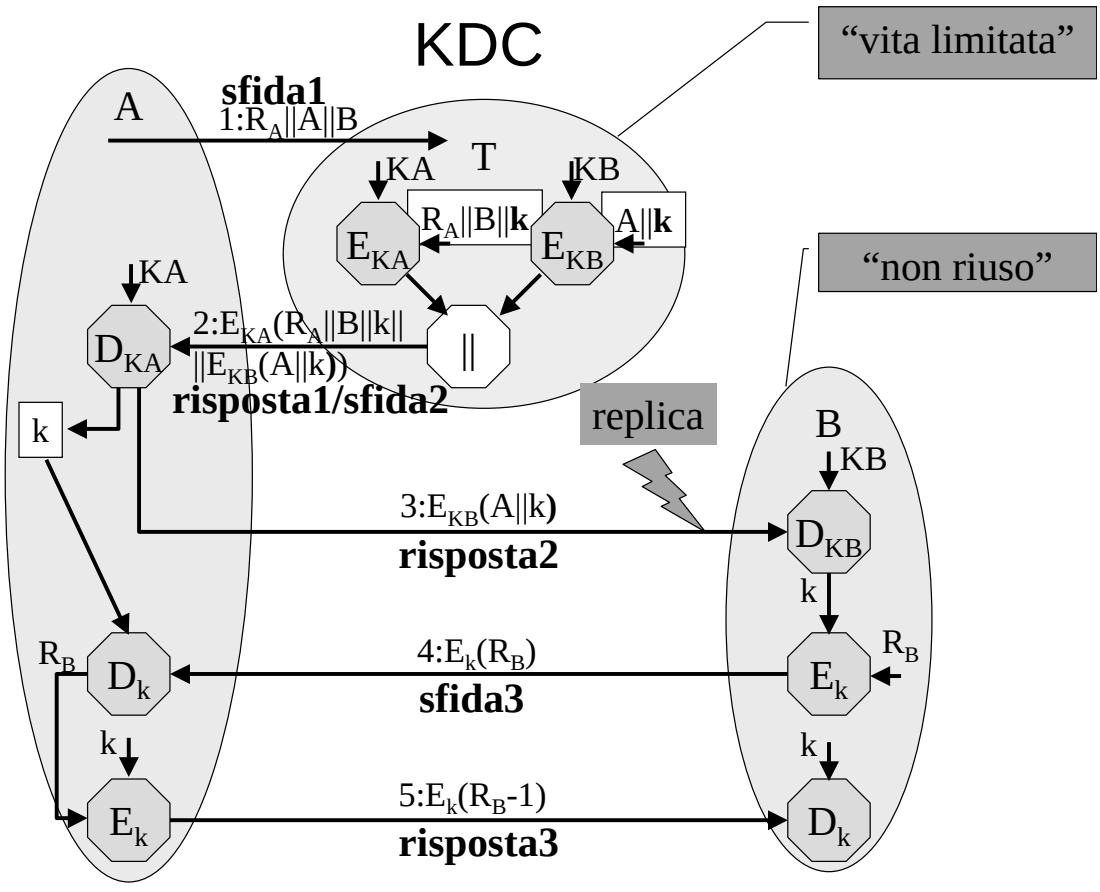


[redacted]

Soluzione: ogni utente concorda la sua chiave con una terza parte

L'Autorità per la distribuzione chiavi

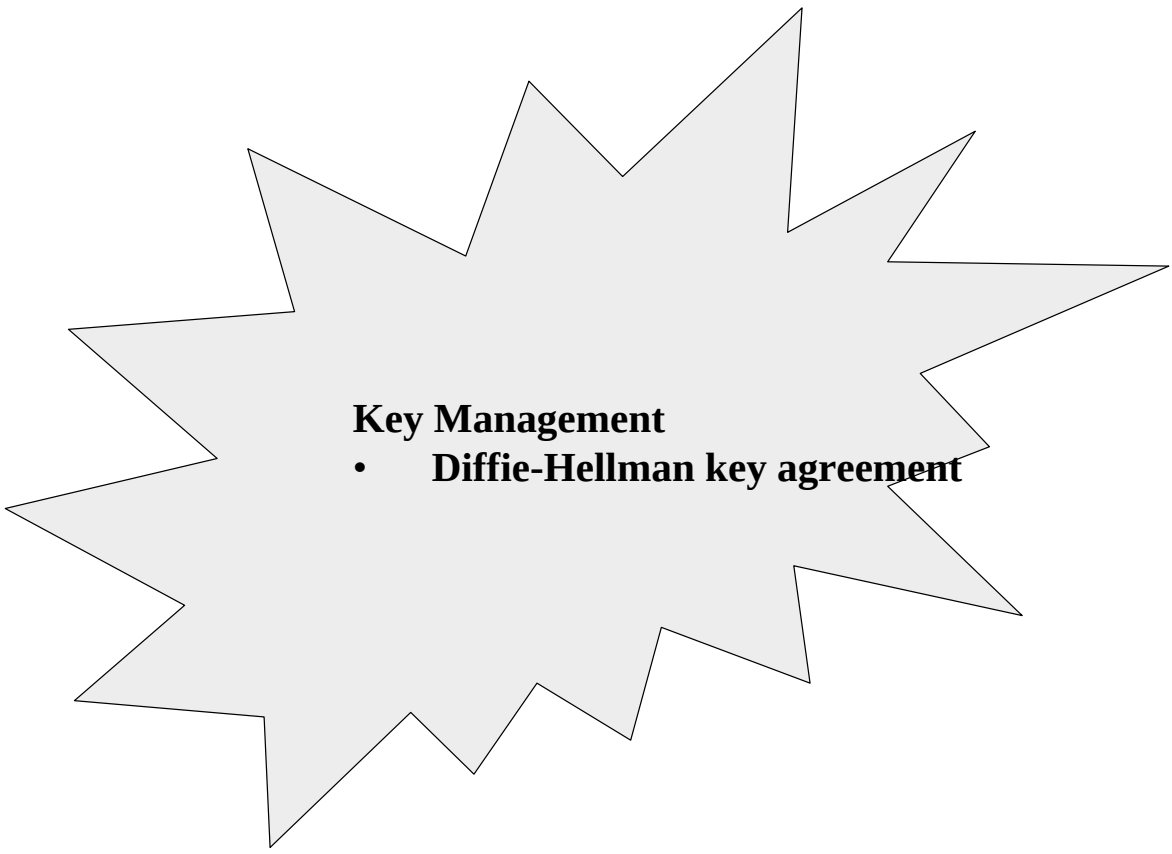




Problemi di KDC

- On-line
- Collo di bottiglia (n° max di utenti)
- Memoria sicura
- Ente degno di fiducia

KryptoKnight,
Kerberos,
Distributed Computing Environment,
Windows 2000



Il contesto “tutti con tutti”

	Accordi precedenti	Numero di chiavi	Valutazione della realizzabilità
Incontri & Corrieri	SI	Enorme	difficile
Rete mondiale di N KDC	SI	1+N(N-1)/2	difficile
Scambio D-H	NO	1	facile

Algoritmo DH *anonimo* per l’accordo di una chiave di sessione tra gli utenti A e B

Numero primo **p** e *generatore* **g** prefissati e noti

1. Generazione delle chiavi segrete

XA e **XB** scelti a caso > 1 e < p-1

2. Generazione e comunicazione delle chiavi pubbliche

$\mathbf{Y_A = g^{XA} \bmod p}$ e $\mathbf{Y_B = g^{XB} \bmod p}$

3. Calcolo della chiave del Cifrario simmetrico

$\mathbf{K_A = Y_B^{XA} \bmod p = (g^{XB})^{XA} \bmod p}$

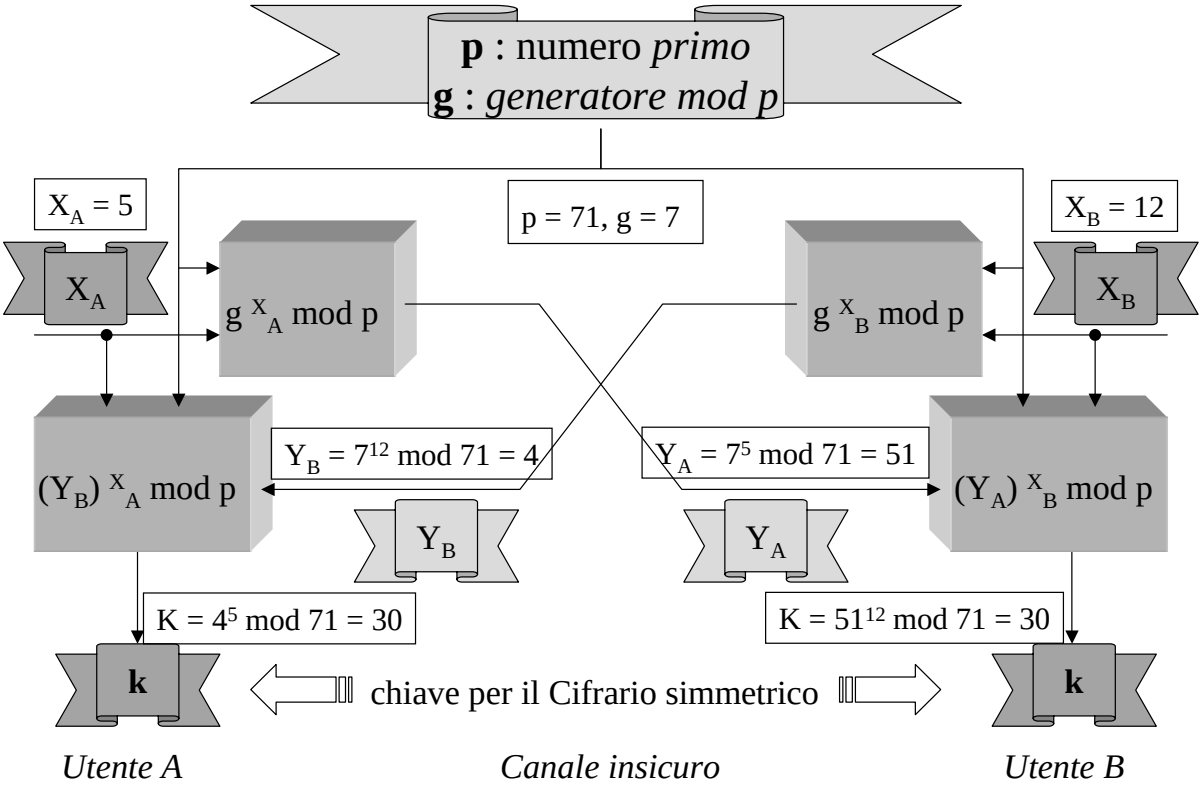
$\mathbf{K_B = Y_A^{XB} \bmod p = (g^{XA})^{XB} \bmod p}$

$$\mathbf{K_A = K_B}$$

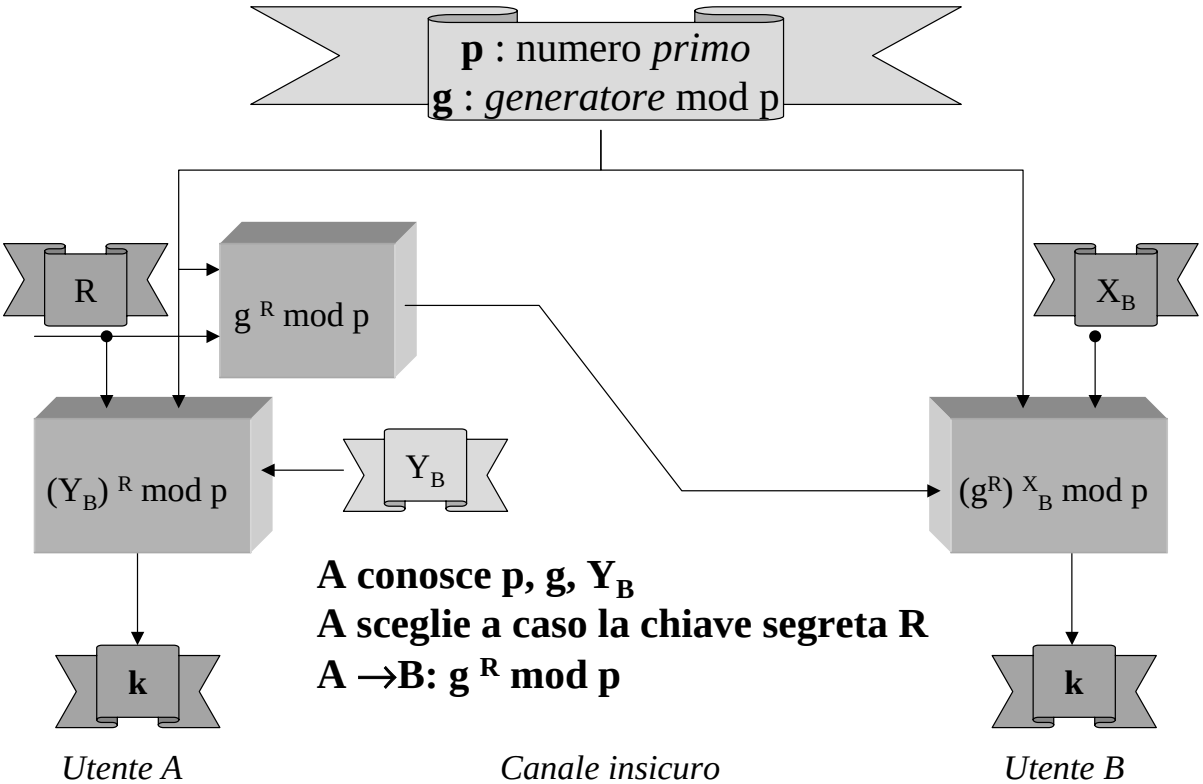
La dimensione è grande (quella di p): occorre scegliere k

DH anonimo: l’origine di Y non è attestata

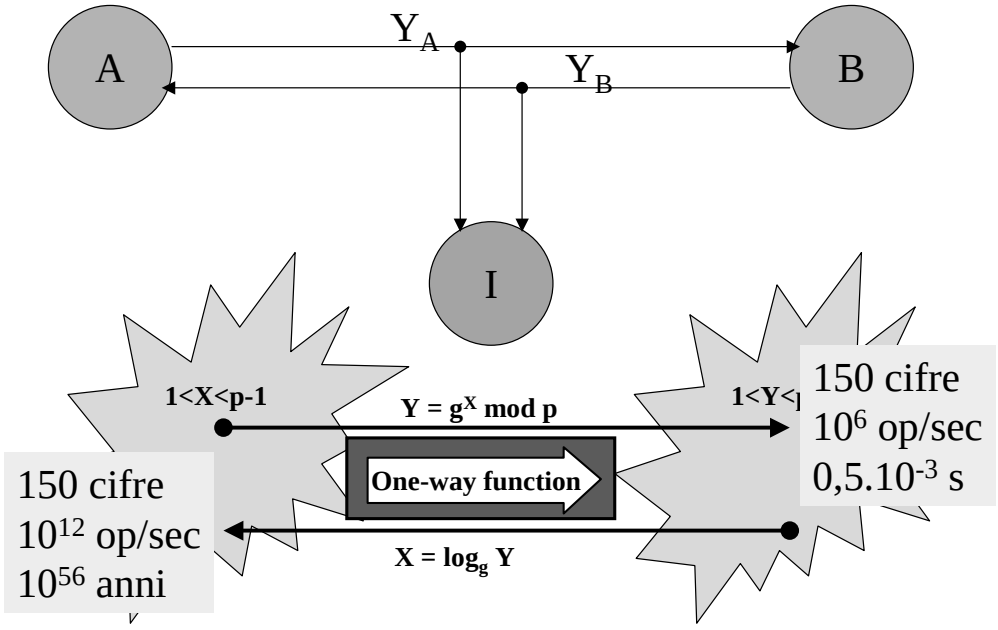
Lo scambio di Diffie-Hellman



Variante DH/ElGamal



Sicurezza dello scambio DH



P1: problema (difficile) del logaritmo discreto su un campo di Galois
" Dato in primo **p**, un generatore **g** ed un intero $\mathbf{c} \in \mathbf{Z^*_p}$, trovare l'intero **x**, $\mathbf{1 \leq x \leq p-2}$, tale che $\mathbf{g^x \bmod p = c}$