

# Guardiamo ora cosa succede...



- ◆ La malefica Crudelia interviene, e fa la seguente cosa: rimanda uno o più dei messaggi
- ◆ Quindi certi messaggi arrivano due (o più) volte a Bob
- ◆ In certi contesti non cambia nulla, semplicemente abbiamo ripetuto quello che avevamo già detto

# Replay attack!!



- ◆ Esempio:  
transazioni finanziarie
- ◆ Immaginate di comprare qualcosa su un e-shop, ad esempio un frigorifero
- ◆ Qualcuno vi fa un replay attack →  
invece di averne comprato uno,  
ne avete comprati trenta!



??

◆ MMORPG !







0 HP 1131/1297  
TP 1540/1812

Lv200

Lil' Kim

Lv200

Usiel

Lv200

Nalsuko

Lv200

Enishi

15 Grass A

152

Grass Assassin  
Attribute: A.Beast

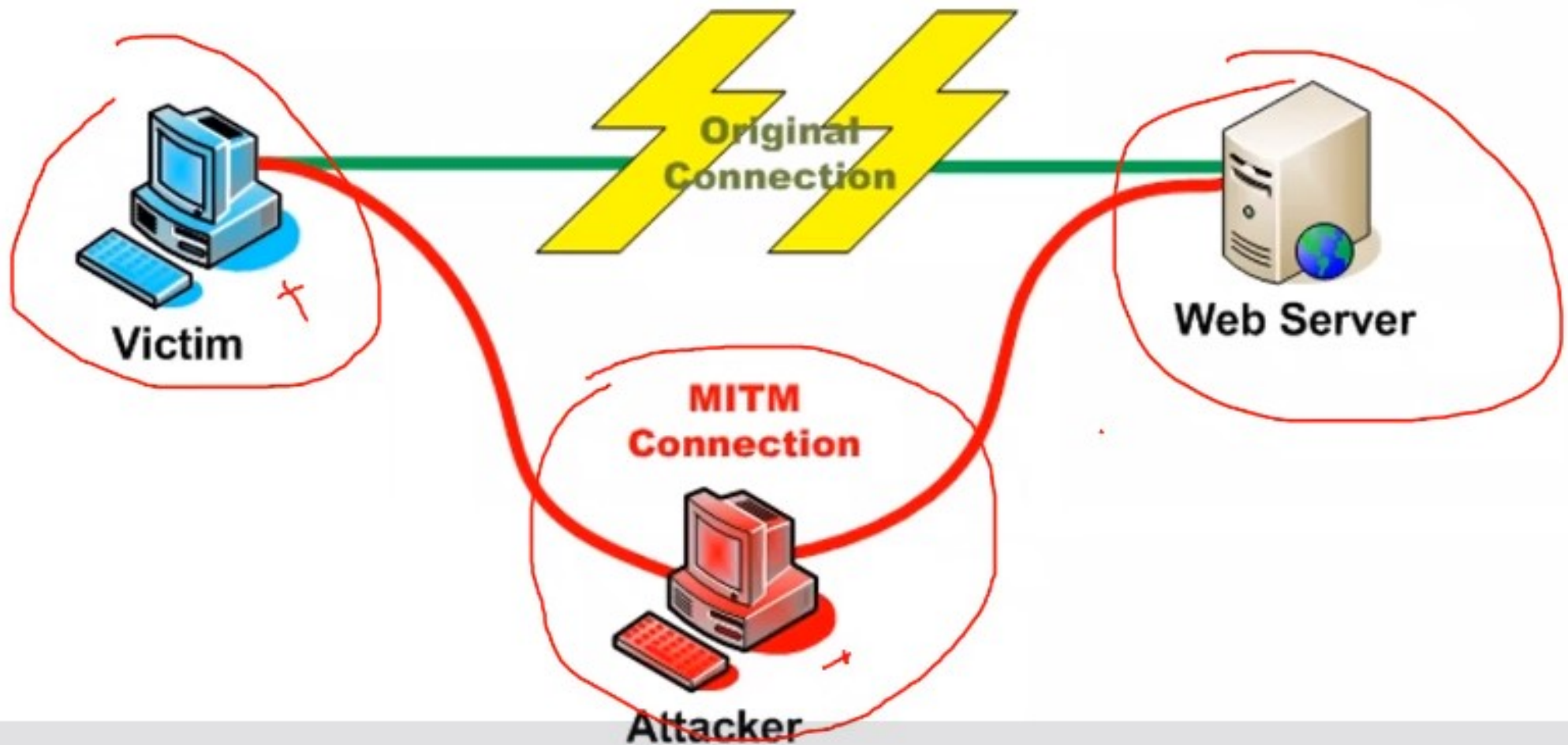
# L'attacco MTM

◆ **MTM** = **M**an in **T**he **M**iddle





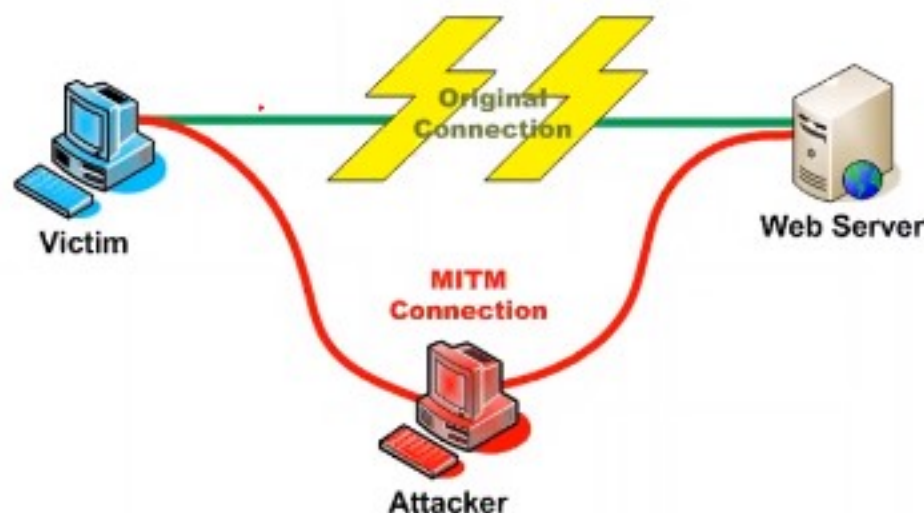
# MTM



# MTM



- ◆ E' un problema fondamentale!
- ◆ Fondamentalmente, rende *impossibile* la gestione della sicurezza senza informazione segreta *pre-condivisa*...

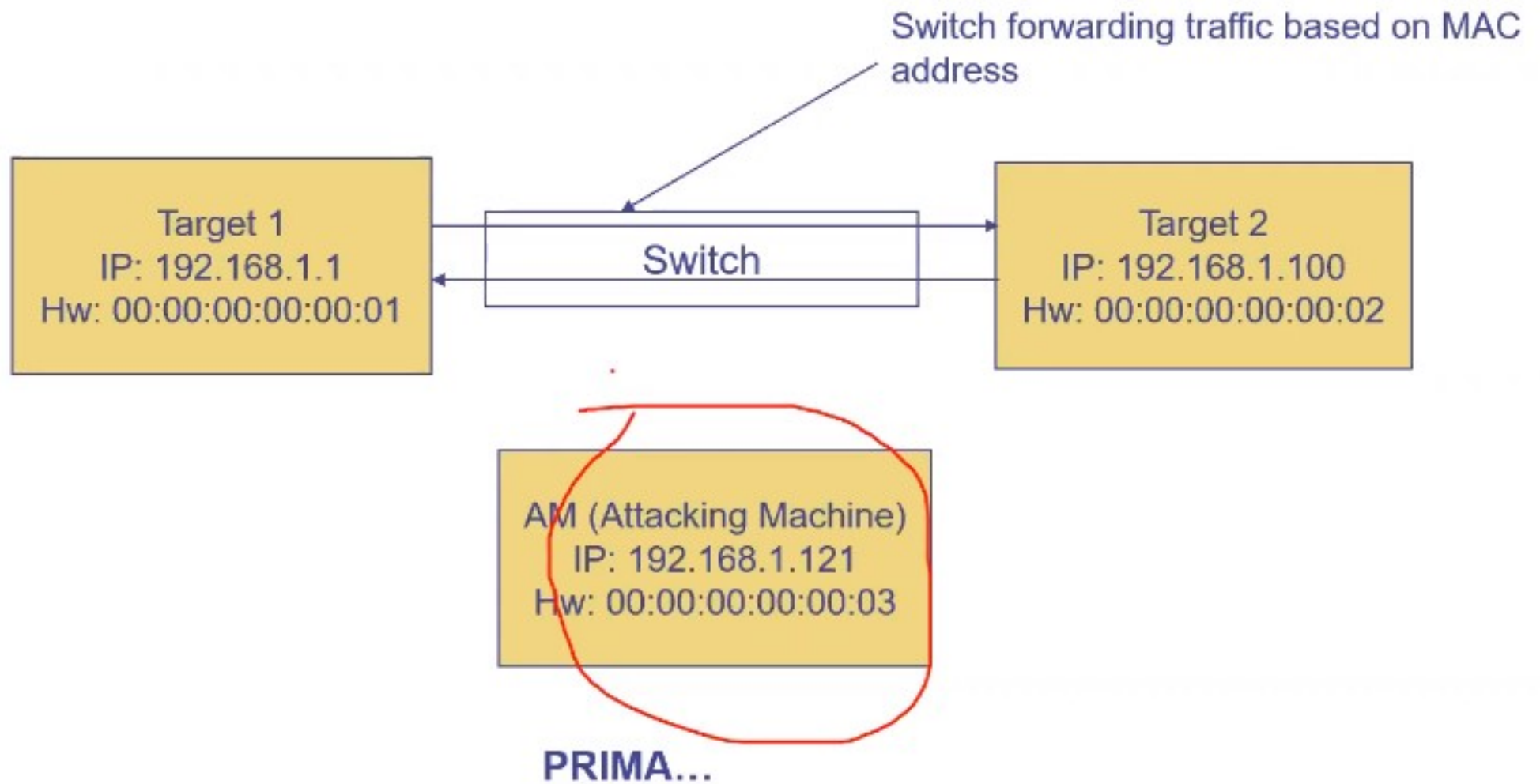


# Esempio: ricordate ARP

- ◆ Corrispondenza indirizzi IP e MAC  
address

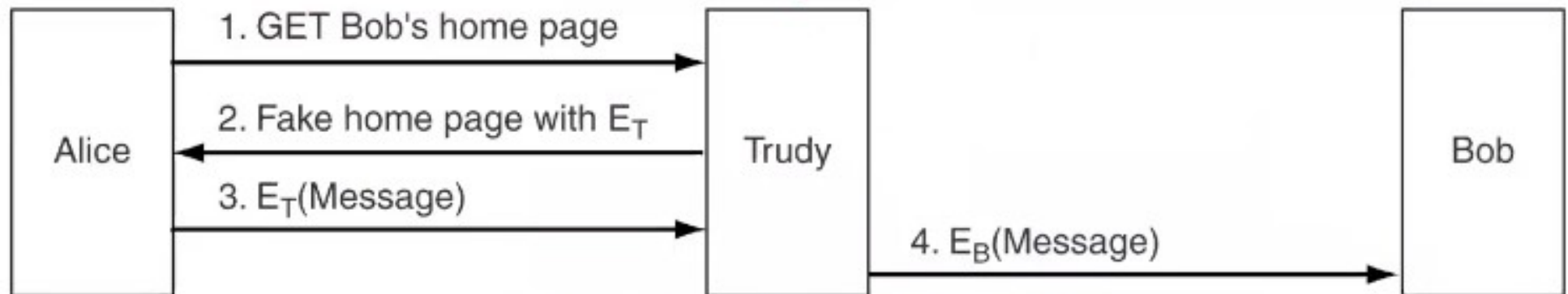






# Esempio: le chiavi pubbliche

◆ Sono suscettibili di MTM, ovviamente





# Servirebbero dei... certificati!

I hereby certify that the public key

19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A

belongs to

Robert John Smith

12345 University Avenue

Berkeley, CA 94702

Birthday: July 4, 1958

Email: bob@superdupernet.com

SHA-1 hash of the above certificate signed with the CA's private key

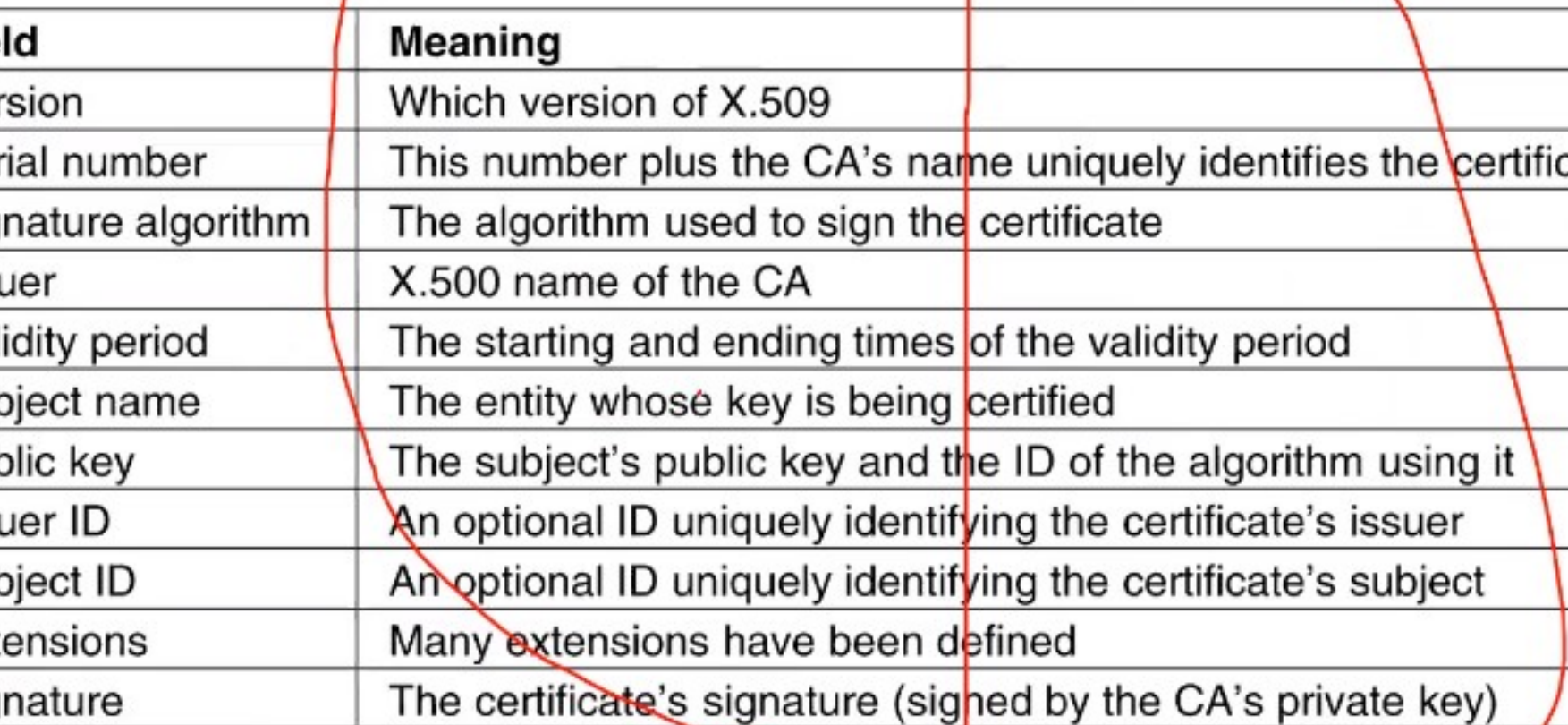
# Serve qualcuno di affidabile...!

- ◆ Una **CA**  
(Certification Authority)

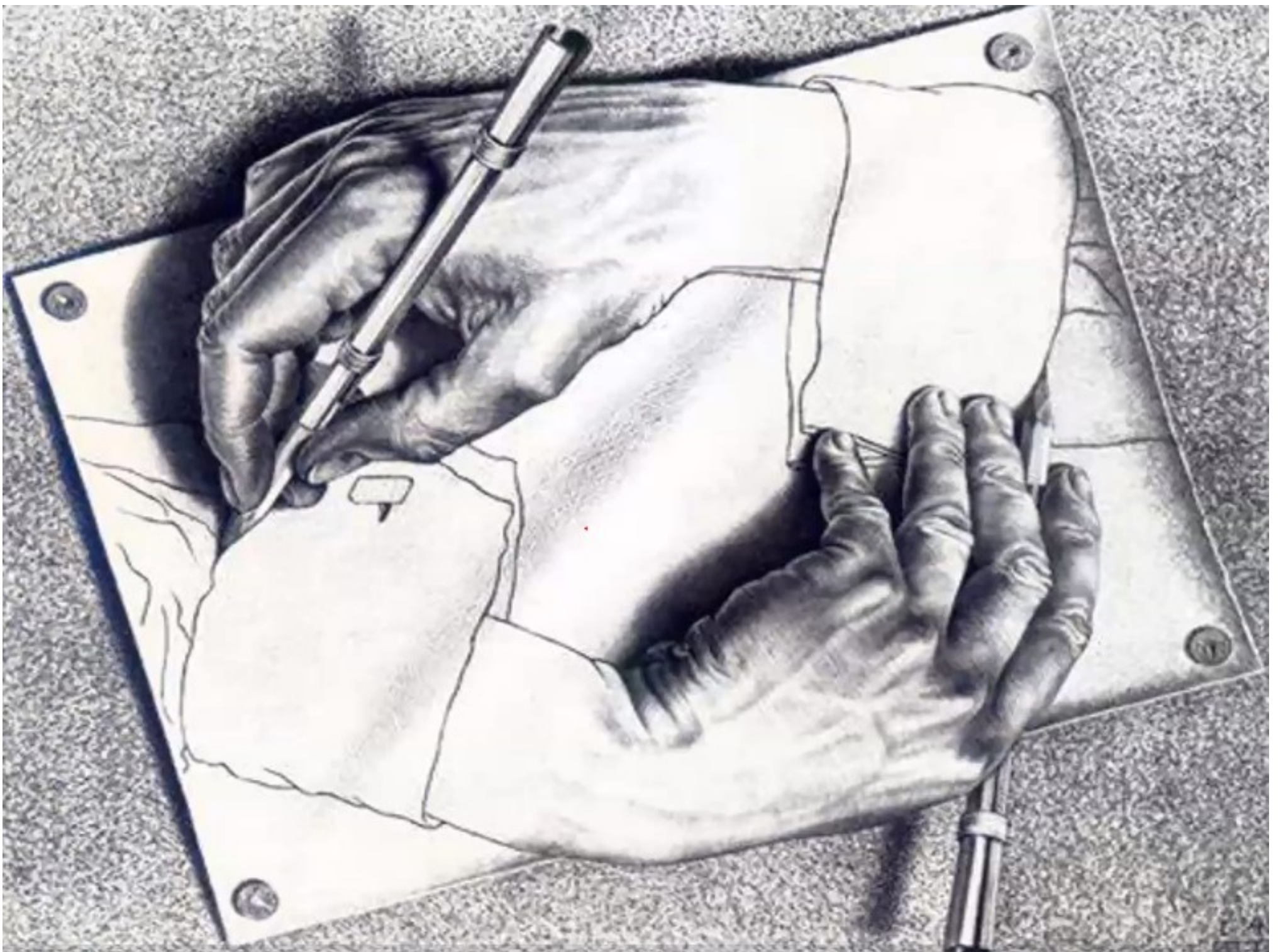




# X.509



Field	Meaning
Version	Which version of X.509
Serial number	This number plus the CA's name uniquely identifies the certificate
Signature algorithm	The algorithm used to sign the certificate
Issuer	X.500 name of the CA
Validity period	The starting and ending times of the validity period
Subject name	The entity whose key is being certified
Public key	The subject's public key and the ID of the algorithm using it
Issuer ID	An optional ID uniquely identifying the certificate's issuer
Subject ID	An optional ID uniquely identifying the certificate's subject
Extensions	Many extensions have been defined
Signature	The certificate's signature (signed by the CA's private key)





Vediamo altri attacchi...



# L'attacco smurf

- ◆ Ad esempio, qualcuno manda dei pacchetti ICMP chiedendo l'echo
- ◆ Anche detto il ***ping of death***





## In generale...

- ◆ ... questo tipo di attacchi rientra nella categoria del **DoS** (*denial of service attack*)
- ◆ Cioè, grosso modo, quando chi attacca supera le risorse disponibili di chi riceve



# Modalità reverse: l'attacco IP spoofing

- ◆ L'IP spoofing si basa sul fatto che IP non ha alcuna sicurezza
- ◆ Quindi quello che possiamo fare è ad esempio ***scrivere un altro mittente***
- ◆ Perché mai dovremmo farlo?

# Per fare DDos...:

- ◆ Ricordate il ***ping of death***... vi basta ora inviare una richiesta ICMP di echo a tantissime macchine, usando come mittente la macchina da attaccare... (!!)

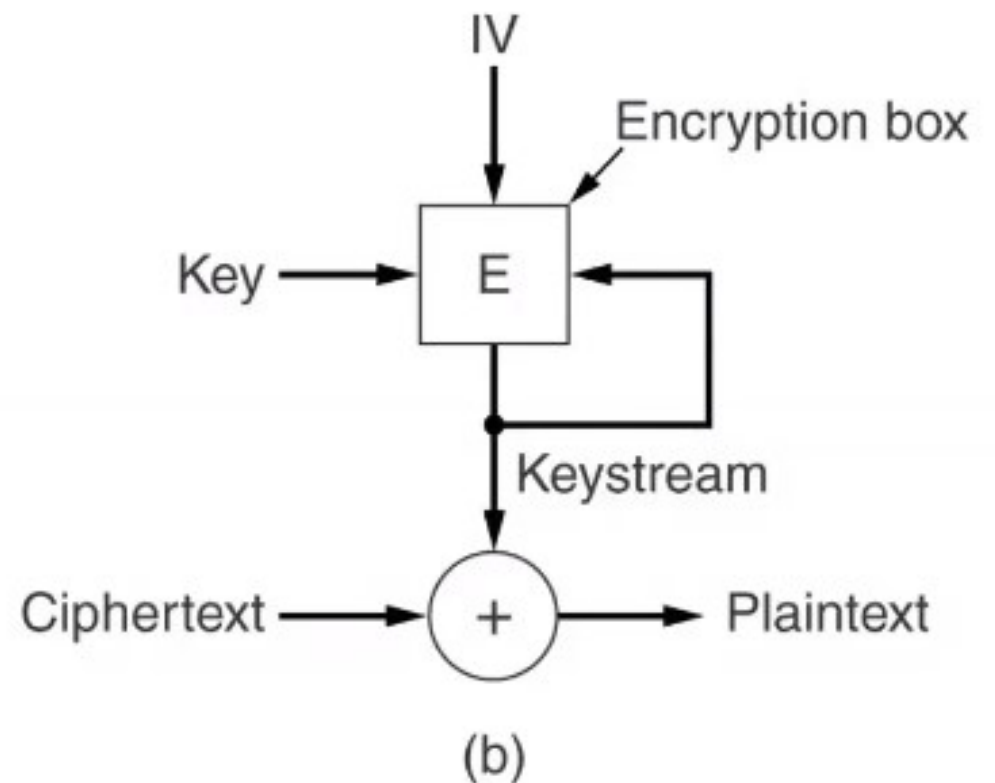
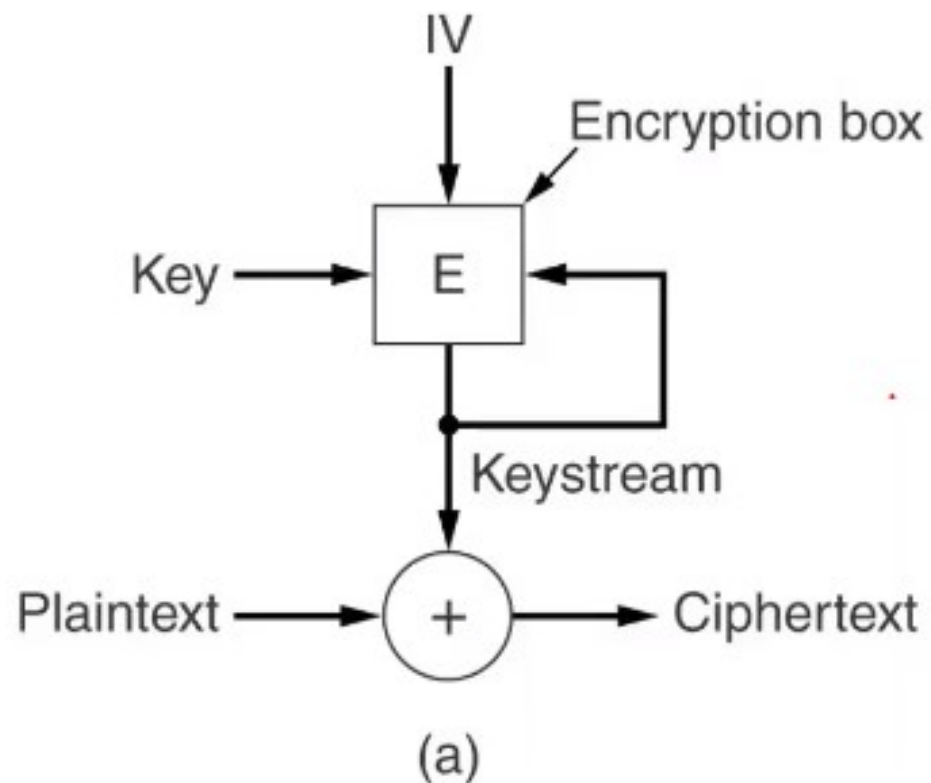




# WEP

- ◆ Wired Equivalent Privacy
- ◆ Funziona usando encrypting a ***chiave simmetrica***
- ◆ Usa un block cipher chiamato RC4 (dove la R qui sta sempre per Rivest)
- ◆ Chiaramente deve proteggersi dal problema dell'Electronic Book Mode → usa una tecnica di mode chaining

# Lo stream cipher!



# Problema...

- ◆ Sociale: passphrase da 8-32 caratteri ASCII → moltissimi usano passphrases corte e simili a parole di dizionario, mai veramente casuali
- ◆ Quindi, chiavi suscettibili di attacchi di tipo ***dictionary***





## 2004: WPA2 / 3

- ◆ Derivato dallo standard **802.11i**
- ◆ Usa **CCMP** (**Counter Mode with Cipher Block Chaining Message Authentication Code Protocol**), basato su **AES**
- ◆ Chiave simmetrica da 128 bits, e blocchi sempre di 128 bits.



"Return of the caveman"...?





# Potenza di Calcolo?





# Jaguar!

- ◆ Il piu' potente supercomputer al mondo!
- ◆ Della Cray Corporation  
(in forza agli Oak Ridge National Laboratory nel Tennessee)
- ◆ **224256** processori X86 Opteron (!!)



# Jaguar!

- ◆ Il piu' potente supercomputer al mondo!
- ◆ Della Cray Corporation (in forza agli Oak Ridge National Laboratory nel Tennessee)
- ◆ **224256** processori X86 Opteron (!!)
- ◆ Potenza: **1,75 petaflops**  
(17500000000000000 FLOPS)



# Ottobre 2010...



- ◆ Tianhe-1a
- ◆ In forza al National University of Defense Technology (NUDT), a Tianjin
- ◆ Potenza: **2,507 petaflops (!!)**



# Jaguar contro Tiahne-1a

- ◆ Jaguar:  
**224256** processori Opteron
- ◆ Tiahne-1a: **7168** "unità" (!!!)
- ◆ Che razza di unità sono...???
- ◆ Dotazione di ogni unità:
- ◆ **Un** processore Xeon X5670



# GPU NVIDIA Tesla M2050 "Fermi"

- ◆ Simile alla linea "consumer" della Geforce GTX 470
- ◆ **3 GB** di memoria RAM
- ◆ **448 cores CUDA**



# Capite quindi...

- ◆ Come l'attacco "return of the caveman" sia solo questione di tempo, quando le schede grafiche scenderanno di prezzo e saranno sempre più potenti... (!!)





Gennaio 2011...

- ◆ Thomas Roth usa il servizio di Amazon **Elastic Computer Cloud (EC2)**



# Configurazione macchina EC2

- ◆ 67 processori  
quad-core Xeon X5570
- ◆ 22Gb RAM
- ◆ 1,7 Terabyte spazio disco
- ◆ ...e due GPU NVIDIA Tesla M2050 "Fermi" !



# Risultato?

- ◆ Potenza dell'attacco:
- ◆ 400000 passwords al secondo
- ◆ → Riesce a **craccare WPA** in circa **20 minuti** (e promette di farlo in **6 minuti** migliorando il codice)
- ◆ Costo dell'affitto? Circa **\$1.68**





# La Soluzione **Definitiva??**

## ◆ **Security Mantra:**

*Il solo modo per avere  
veramente sicurezza è di  
non essere connessi  
alla rete!!!*



# Morale:

- ◆ Un punto debole si trova sempre prima o poi
- ◆ → Il solo modo per avere veramente sicurezza è ***pianificare sempre per il caso peggiore...!***

