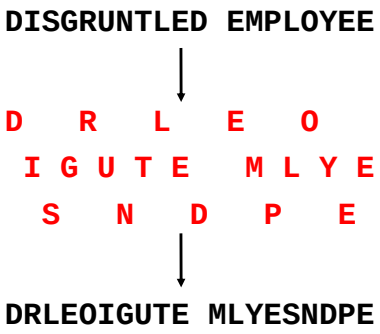
Introduzione alla Crittografia

Tipologie di Base di Crittografia

- Transposition ciphers – la cifratura avviene mediante una nuova disposizione dei bit / caratteri
- Substitution ciphers – bit / caratteri / blocchi vengono sostituiti da altri

Cifratura "Rail-Fence"

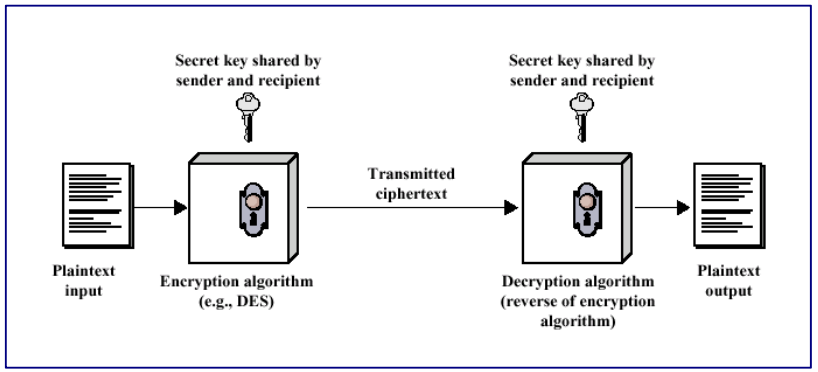


Metodi di Crittografia

- La sicurezza nella stragrande maggioranza dei casi è basata su crittografia
- Due approcci fondamentali:
  - Crittografia convenzionale, o crittografia simmetrica
  - Crittografia a chiave pubblica, o crittografia asimmetrica

Crittografia Convenzionale

Modello di Crittografia Convenzionale



Crittografia Convenzionale

- È stata l'unica forma di crittografia sino ai tardi anni '70 del XX secolo
- Ha una lunga storia

Crittografia Convenzionale

- Gli algoritmi sono caratterizzati da:
  - Plaintext: I dati originali
  - Encryption algorithm: svolge le trasformazioni sul plaintext
  - Secret key: Input all'algoritmo; le trasformazioni dipendono da questa
  - Ciphertext: messaggio prodotto come output; dipende da plaintext e secret key
  - Decryption algorithm: inverso dell'algoritmo di Encryption; Usa ciphertext e secret key per produrre il plaintext originale

Conventional Encryption

- Più formalmente, le 5 componenti sono
  - Un Plaintext message space, $\mathcal{M}$
  - Una famiglia di trasformazioni di codifica, E_K: $\mathcal{M} \rightarrow \mathcal{C}$, dove $K \in \mathcal{K}$
  - Un key space, $\mathcal{K}$
  - Un ciphertext message space, $\mathcal{C}$
  - Una famiglia di trasformazioni di decodifica, D_K: $\mathcal{C} \rightarrow \mathcal{M}$, dove $K \in \mathcal{K}$

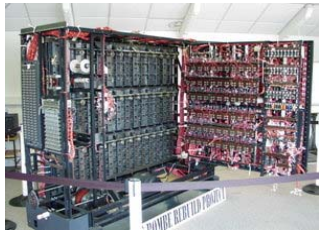
Requisiti e Debolezze

- Requisiti
  - Un forte algoritmo di crittografia
  - Processi sicuri per il mittente e il ricevente per ottenere le secret key
- Metodi di Attacco
  - Cripto analisi
  - Brute force

Cryptanalysis

- The process of attempting to discover the plaintext or key

Alan Turing broke the Enigma Code in WWII



Cryptanalysis

- La sicurezza dipende dalla chiave
  - Non dalla segretezza dell'algoritmo
- Il problema principale è mantenere la sicurezza della chiave

Sistemi Crittografici

- Tipo della trasformazione
  - Per sostituzione / trasformazione
  - Nessuna perdita di informazione (reversibilità)
- Numero delle chiavi usate
  - Una chiave per sistemi simmetrici
  - Due chiavi per sistemi asimmetrici
- Elaborazione del plaintext
  - Per blocco
  - Per stream

Attacks On Encrypted Msgs

Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Sicurezza computazionale

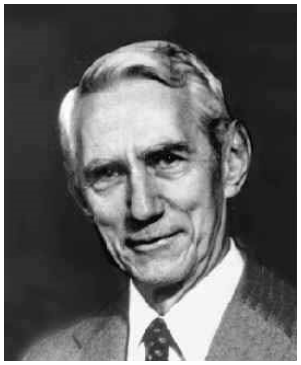
- Il costo richiesto per violare la codifica deve eccedere il valore dell'informazione cifrata
- Il tempo necessario per violare la codifica deve eccedere il tempo di vita utile dell'informazione cifrata

Exhaustive Key Search

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years

Brute Force with massively parallel processors

Claude Shannon



- *A Mathematical Theory of Communication* (1948), outlining what we now know as Information Theory
- Described ways to measure data using the quantity of disorder in any given system, together with the concept of entropy
- *The Magna Carta of the information age*
- Retired at age 50

Claude Shannon

- Concetto di entropy dell'informazione, derivato da quello della termodinamica
- Second law of thermodynamics – **entropy** is the degree of randomness in any system
- Levando l'entropia da un messaggio, questo può essere accorciato senza perdita semantica
- Shannon ha dimostrato che in una conversazione con rumore il segnale può sempre essere inviato senza distorsione

Claude Shannon

- If the message is encoded in such a way that it is **self-checking**, signals will be received with the same accuracy as if there were no interference on the line
- A language has a built in **error-correcting code**
- http://cm.bell-labs.com/cm/ms/what/shannonday
- http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html

Information Theory

- Information theory measures the **amount of information** in a message by the average number of bits needed to encode all possible messages in an optimal encoding
- GENDER field in a database: only one bit of information (Male:0; Female:1)
- Encoded in ASCII – more space, but *no more information*

Information Theory

- **Amount of information** in a message is formally measured by the **entropy** of the message
- **Entropy** is a function of the probability distribution over the set of all possible messages

Information Theory

- **Entropy** of a given message is defined by the weighted average over all possible messages X:

$$H(X) = \sum_X p(X) \log_2\left(\frac{1}{p(X)}\right)$$

Information Theory Example

p(male) = p(female) =1/2, then

$$H(X) = \frac{1}{2}(\log_2 2) + \frac{1}{2}(\log_2 2)$$

$$= \frac{1}{2} + \frac{1}{2} = 1$$

- There is 1 bit of information in the GENDER field of a database

Information Theory

- Text files can be reduced by about 40% without losing information
- Because *1/p(x)* decreases as *p(x)* increases, an ***optimal encoding*** *uses short codes for frequently occurring messages; longer codes for infrequent*
- *Morse code*
  E •, T –, J • – – –, Z – – • •

Information Theory

- The entropy of a message measures its **uncertainty**. The number of bits that must be learned when the message is hidden in ciphertext
- **English** is a highly **redundant**
- occurring frequently => ocrng frq

English Redundancy

- Delete vowels and double letters

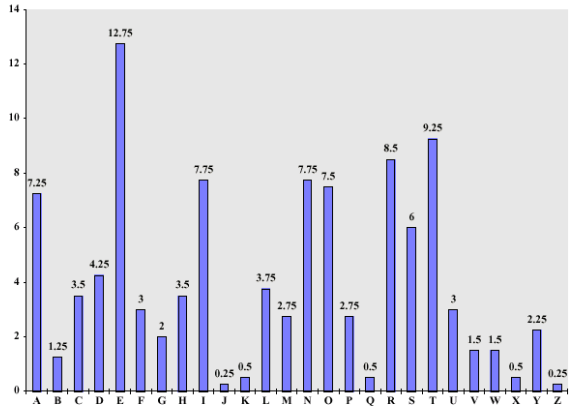
mst ids cn b xprsd n fwr ltrs,
bt th xprnc s mst nplsnt

Simple Cryptanalysis

CIPHERTEXT:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

Letter Frequency In the English Language



Simple Cryptanalysis

PLAINTEXT:

IT WAS DISCLOSED YESTERDAY THAT SEVERAL INFORMAL BUT DIRECT CONTACTS HAVE BEEN MADE WITH POLITICAL REPRESENTATIVES OF THE VIET CONG IN MOSCOW

20th Century Encryption

- 20's & 30's bootleggers made heavy use of cryptography
- FBI create an office for code-breaking
- Japanese Purple Machine
- German Enigma Machine
- Navajo Code Talkers - Windtalkers

Hedy Lamarr

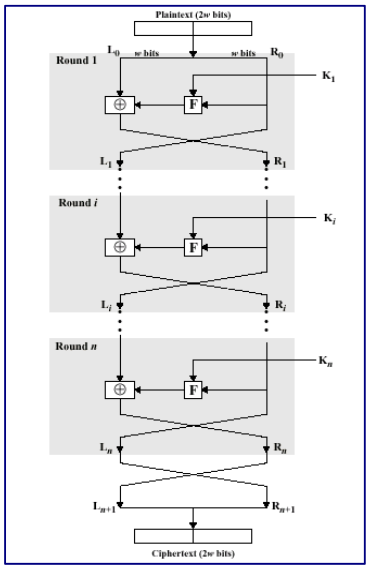
- 1941, Lamarr and composer George Antheil received a patent for their invention of a classified communication system that was especially useful for submarines
- It was based on radio frequencies changed at irregular periods that were synchronized between the transmitter and receiver
- **Spread Spectrum** – wireless devices

Struttura del Cifrario di Feistel

- Horst Feistel of IBM, 1973
- Input è un blocco plaintext block lungo $2w$ bit (di solito 64) e una chiave K
- Il blocco è diviso in due metà, L_0 e R_0
- Ogni iterazione i ha gli input L_{i-1} e R_{i-1}, ottenuti dalla iterazione i-1, con la sottochiave K_i
- Si effettua una sostituzione sulla metà sinistra dei dati
- **Round function** F è applcata alla metà destra, poi combinata in XOR con la sinistra

Feistel Cipher Structure

Things to consider:
-Block size (64)
-Key Size (128)
-# of rounds (16)
-SubKey Generation
-Round function

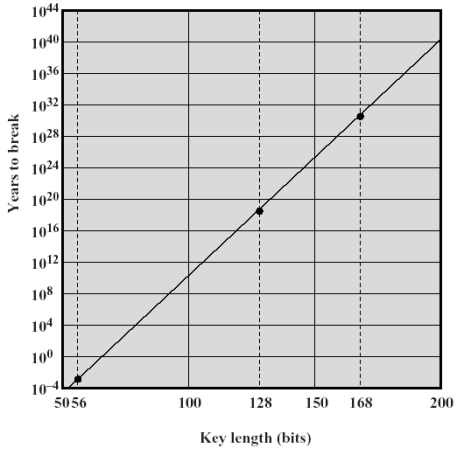


Data Encryption Standard (DES)

- Adottato nel 1977, da NBS(NIST), riconfermato per 5 anni nel 1994
- Plaintext è lungo 64 bit (o blocchi di 64 bit), la chiave è lunga 56 bit
- Sono effettuate 16 iterazioni, ciascuna produce un risultato intermedio che è input per la successiva
- DES è ora considerato troppo facile da violare per essere un metodo utile

Strength of DES

- Concerns about the algorithm itself
- Concerns about 56-bit key – this is the biggest worry

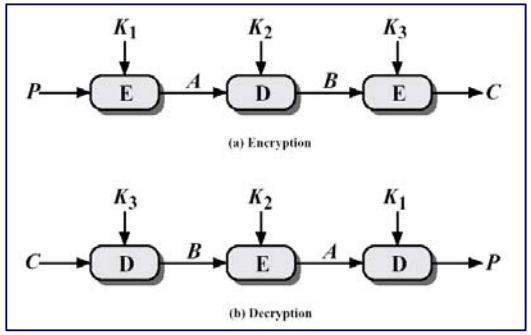


Strength of DES

- DES è l'algoritmo di crittografia più studiato
- Nessuno ne ha scoperto debolezze fatali
- Nel 1998 è stato violato
- Solution: Use a bigger key

Triple DES

$C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]$



Triple DES

- Alternativo al DES, svolge plurime codifiche con il DES e più chiavi
- Con tre chiavi distinte, 3DES ha una chiave effettiva di 168 bits, ed è esenzialmente immune da attacchi a forza bruta
- Backward compatible with DES
- Principal drawback of DES is that the algorithm is relatively sluggish in software

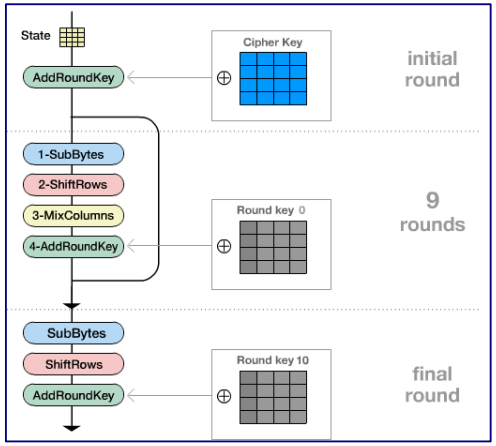
Advanced Encryption Standard

- NIST call for proposals in 1997
- Nov, 2001 – **Rijndael** [rain´ dow]
- Symmetric block cipher (128 bits) and key lengths 128, 192, 256
- Two Flemish cryptographers: Joan Daeman and Vincent Rijmen

Overview of AES

4Transformations:

- Substitute Bytes
- Shift Rows
- Mix Columns
- Add Round Key



AES URLS

- http://csrc.nist.gov/CryptoToolkit/aes/rijndael/ - NIST AES
- http://www.esat.kuleuven.ac.be/~rijmen/rijndael/ - Rijndael Home Page
- http://www.esat.kuleuven.ac.be/~rijmen/rijndael/Rijndael_Anim.zip - Great Animation

IDEA
International Data Encryption Algorithm

- 1991 by Swiss Federal Institute of Technology
- Uses 128-bit key
- Complex functions replace S-boxes
- Highly resistant to cryptanalysis
- Used in PGP

Blowfish

- 1993 by Bruce Schneier
- Easy to implement; high execution speed
- Variable key length up to 448 bits
- Used in a number of commercial applications

RC5

- 1994 by Ron Rivest, one of the inventors of RSA algorithm
- Defined in RFC2040
- Suitable for hardware and software
- Simple, fast, variable length key, low memory requirements
- High security

CAST-128

- 1997, Entrust Technologies
- RFC 2144
- Extensively reviewed
- Variable key length, 40-128 bits
- Used in PGP

Conventional Encryption Algorithms

Algorithm	Key Size (bits)	Block Size (bits)	Number of Rounds	Applications
DES	56	64	16	SET, Kerberos
Triple DES	112 or 168	64	48	Financial key management, PGP, S/MIME
AES	128, 192, or 256	128	10, 12, or 14	Intended to replace DES and 3DES
IDEA	128	64	8	PGP
Blowfish	variable to 448	64	16	Various software packages
RC5	variable to 2048	64	variable to 255	Various software packages

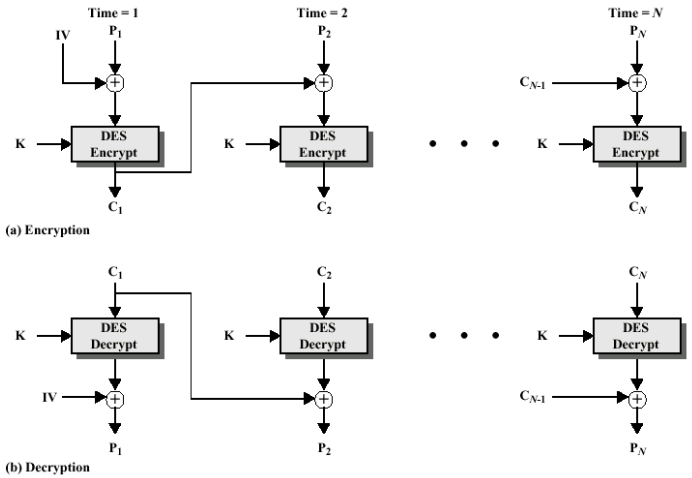
Modalità di Funzionamento per i Cifrari a Blocco

- I cifrari a blocco elaborano **un blocco a n-bit** per volta
- Usa **Electronic Code Book** (ECB)
  - Ogni blocco è codificato con la stessa chiave
  - Considera una entry per ogni possibile pattern di plaintext a 64-bit
  - Più istanze di un blocco producono lo stesso ciphertext
  - Pattern ripetuti sono un problema

Cipher Block Chaining Mode

- Input all'algoritmo è lo **XOR** dell'attuale blocco di plaintext e il blocco precedentemente cifrato
- **Pattern ripetuti** non rappresentano un rischio

Cipher Block Chaining Mode



Cipher Feedback Mode

- Convert DES into a **stream cipher**
- **Eliminates** need to **pad** a message
- Operates in **real time**
- Each character can be **encrypted** and **transmitted immediately**

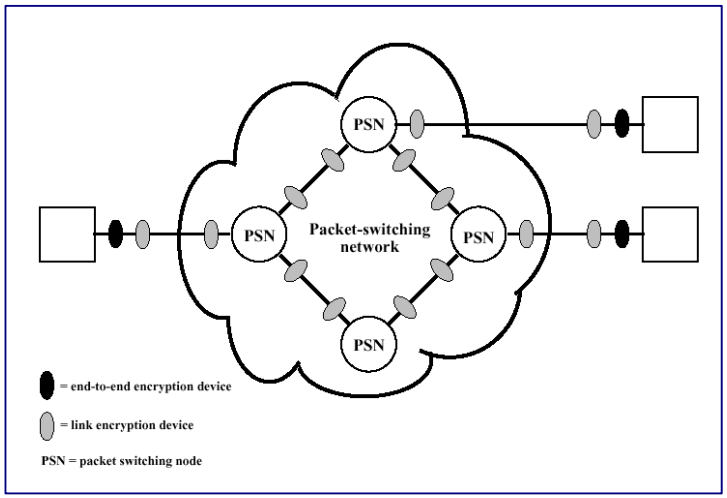
Location of Encryption Devices

- **Link Encryption**
  - Each vulnerable communications link is equipped on both ends with an encryption device
  - All traffic over all communications links is secured
  - Vulnerable at each switch

Location of Encryption Devices

- **End-to-end Encryption**
  - The encryption process is carried out at the two end systems
  - Encrypted data are transmitted unaltered across the network to the destination, which shares a key with the source to decrypt the data
  - Packet headers cannot be secured

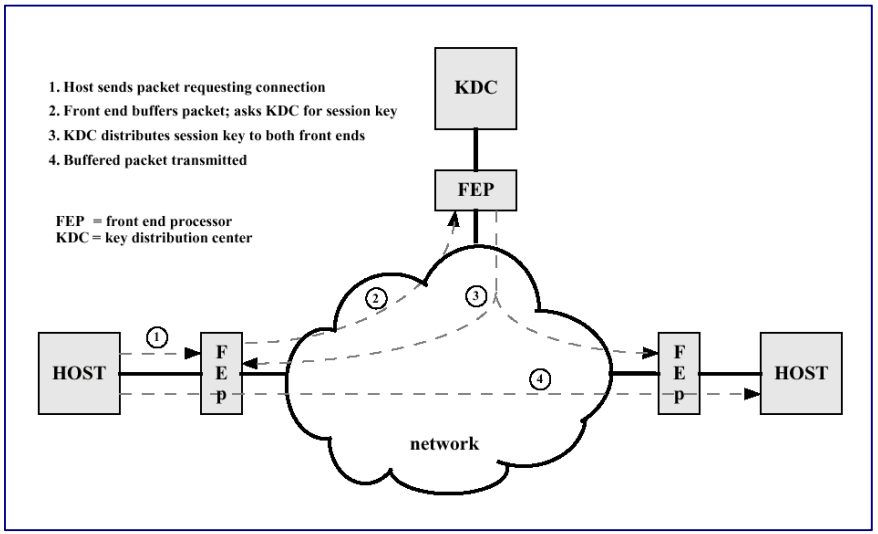
Location of Encryption Devices



Distribuzione delle Chiavi

- **Entrambi i comunicanti** devono conoscere la chiave segreta
- La chiave va cambiata frequentemente
- È necessario una distribuzione manual, oppure un canale terzo codificato
- Tra i più efficaci metodi c'è il **Key Distribution Center** (e.g. Kerberos)

Key Distribution



Network Security

DNS & Addressing

Internet History

- Evolved from ARPANet (Defense Department's Advanced Research Projects Agency Network)
- ARPANet was developed in 1969, and was the first packet-switching network
- Initially, included only four nodes: UCLA, UCSB, Utah, and SRI

NSF and the Internet

- In the 1980s, NSFNet extended packet-switched networking to non-ARPA organization; eventually replaced ARPANet
- Instituted Acceptable Use Policies to control use
- CIX (Commercial Internet eXchange) was developed to provide commercial internetworking

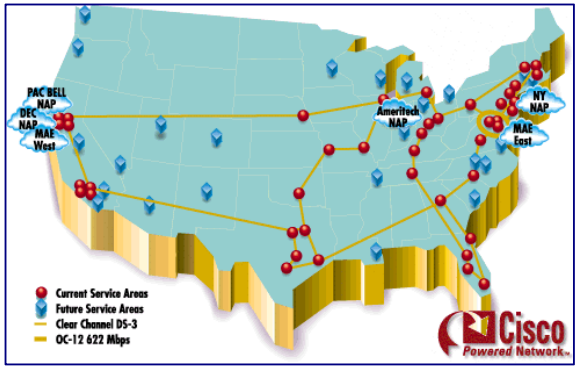
The World Wide Web

- Concept proposed by **Tim Berners-Lee** in 1989, prototype WWW developed at CERN in 1991
- First graphical browser (**Mosaic**) developed by Mark Andreessen at NCSA
- Client-server system with browsers as clients, and a variety of media types stored on servers
- Uses **HTTP** (**H**yper **T**ext **T**ransfer **P**rotocol) for retrieving files

Connecting to the Internet

- End users get connectivity from an ISP (Internet Service Provider)
  - Home users use dial-up, ADSL, cable modems, satellite, wireless
  - Businesses use dedicated circuits connected to LANs
- ISPs use "wholesalers" called network service providers and high speed (T-3 or higher) connections

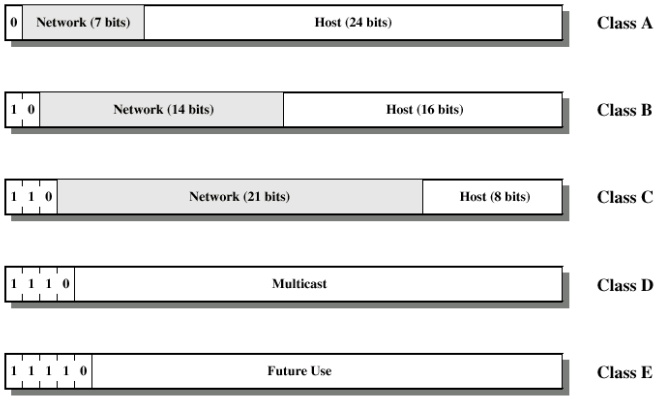
US Internet Access Points



Indirizzamento in Internet

- Indirizzo globale in Internet con 32-bit
- Include identificatori di network e di host
- Notazione decimale con punti
  - 11000000 11100100 00010001 00111001 (binario)
  - 192.228.17.57 (decimale)

Indirizzamento in Internet



Classi di Reti

- Class A: Poche reti, ciascuna con molti host; tutti gli indirizzi cominciano con 0 binario; Range: 1-126
- Class B: numero medio di reti, ciascuna con un numero medio di host; tutti gli indirizzi cominciano con 10 binario; Range: 128-191
- Class C: molte reti, ciascuna con pochi host; tutti gli indirizzi cominciano con 11 binario; Range: 192-223

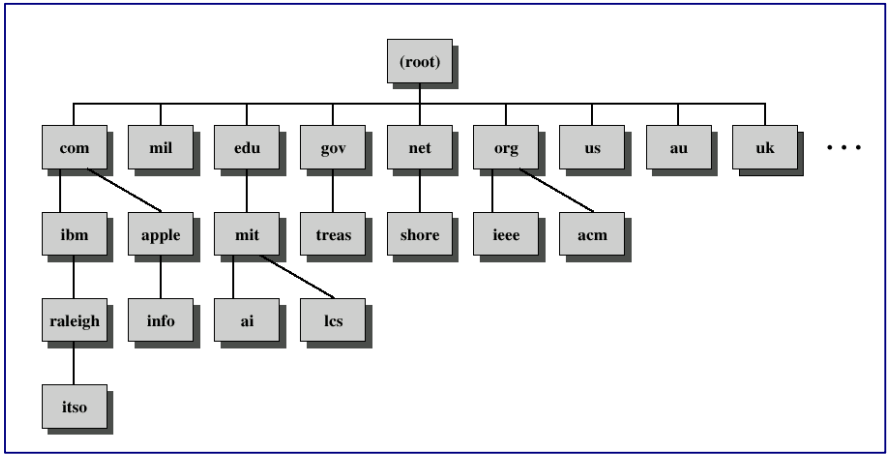
Domain Name System

- 32-bit IP addresses have two drawbacks
  - Routers can't keep track of every network path
  - Users can't remember dotted decimals easily
- **Domain names** address these problems by providing a name for each network domain (hosts under the control of a given entity)

DNS Database

- **Hierarchical database** containing name, IP address, and related information for hosts
- Provides **name-to-address** directory services

Domain Tree



Crittografia a Chiave Pubblica

Recall Security Services

- **Confidentiality** – protection from passive attacks
- **Authentication** – you are who you say you are
- **Integrity** – received as sent, no modifications, insertions, shuffling or replays

Security Attacks

- eavesdropping, monitoring transmissions
- conventional encryption helped here

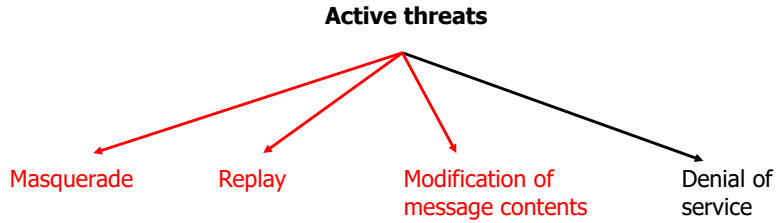
Security Attacks

NEW YORKER

"On the Internet, nobody knows you're a dog."

On the Internet, nobody knows you're a dog
- by Peter Steiner, New York, July 5, 1993

Security Attacks



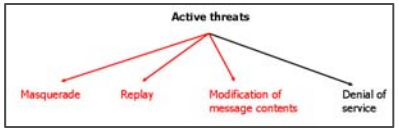
- Message authentication helps prevents these!

Autenticazione di Messaggi

- Procedura che permette ai comunicanti di verificare che i msg ricevuti siano autentici
- Caratteristiche:
  - La sorgente è chi dichiara di esserlo: Evita il *masquerading*
  - I contenuti non sono modificati: Evita il *message modification*

Uso della Crittografia Convenzionale

- Solo mittente e destinatario condividono la chiave
- Si inserisce nel msg un time stamp
- Si inserisce un codice di identificazione degli errori e un numero di sequenza



Autenticazione senza Crittografia

- Si appende un tag di autenticazione al msg
- I messaggi sono letti indipendentemente dalla funzione di autenticazione
- No message confidentiality

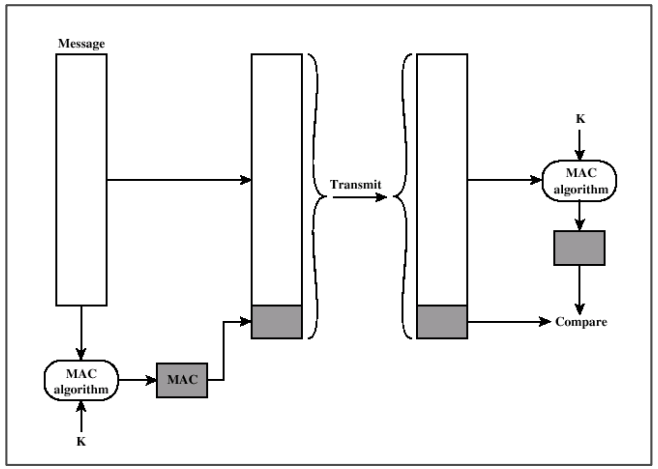
Autenticazione senza Confidenzialità

- Applicazioni che mandano msg in broadcast – solo un destinatario deve controllare l'autenticazione
- Troppo pesante da decrittare – verifica casuale dell'autenticazione
- File – verificati quando è richiesto

Message Authentication Code

- Message Authentication Code (MAC) – usa una chiave segreta per generare un piccolo blocco di dati da appendere al msg
- Se A e B condividono una chiave K_{AB}
- $MAC_M = F(K_{AB},M)$

Message Authentication Code



Message Authentication Code

- Il destinatario è certo che il messaggio:
  - non è stato modificato
  - è stato inviato dal mittente indicato
- Il sequence number assicura che il messaggio è costituito dai pck nella sequenza indicata

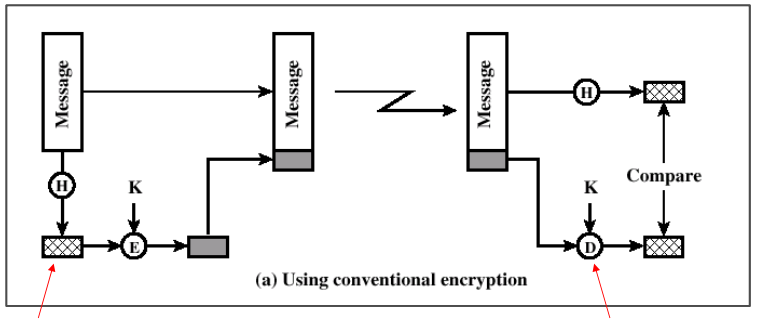
Message Authentication Code

- Viene usato il DES
- Requisito: NON reversibilità
- Checksum

One Way Hash Function

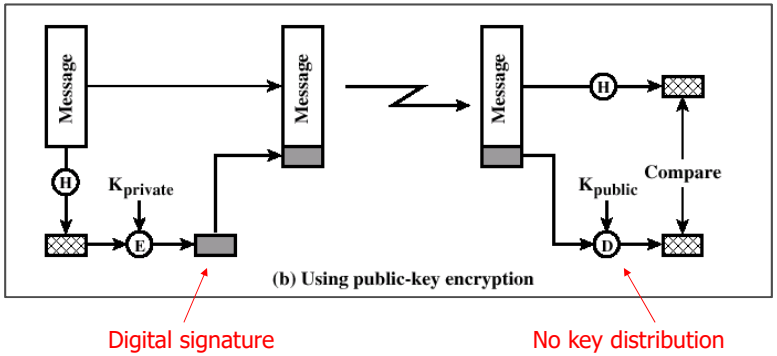
- Una Hash function accetta un messaggio di dimensione variabile M come input e produce un message digest $H(M)$ a dimensione fissa come output
- No secret key as input
- Message digest è inviato con il messaggio per l'autenticazione
- Produce una fingerprint del messaggio

One Way Hash Function



Authenticity is assured

One Way Hash Function



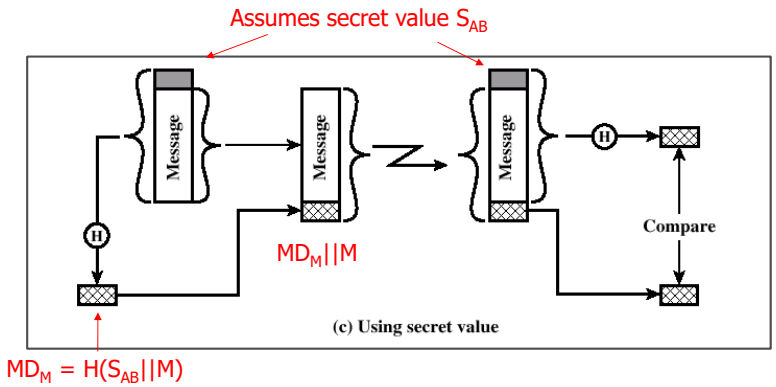
Less computation since message does not have to be encrypted

One Way Hash Function

Ideally We Would Like To Avoid Encryption

- Encryption software is slow
- Encryption hardware costs aren't cheap
- Hardware optimized toward large data sizes
- Algorithms covered by patents
- Algorithms subject to export control

One Way Hash Function



No encryption for message authentication
Secret value never sent; can't modify the message
Important technique for **Digital Signatures**

Requisiti per Hash Functions

- *H* deve poter essere applicata a bocchi di qualsiasi dimensione
- Produce output di lunghezza prefissata
- *H(x)* deve essere facile da calcolare
- Per ogni codice *h* deve essere computazionalmente difficile/impossibile trovare una *x* tale che *H(x)=h* (Proprietà di unidirezionalità)

Requisiti per Hash Functions

- Per ogni blocco x deve essere computazionalmente difficile/impossibile trovare una *y≠x* tale che *H(y)=H(x)* (Resistenza debole alle collisioni)
- Deve essere computazionalmente impossibile trovare una coppia (x,y) tale che *H(x)=H(y)* (Resistenza forte alle collisioni)

Hash Function Semplici

- Input: sequenza di blocchi da n-bit
- Elaborazione: un blocco alla volta, che produce una hash function di n-bit
- Semplicità: Applicazione di XOR bit-a-bit per ogni blocco

$$C_i = b_{i1} \oplus b_{i2} \oplus \cdots \oplus b_{im}$$

- Tale funzione produce un semplice bit di parità per ogni posizione dei bit
  - È nota come controllo di ridondanza longitudinale

Bitwise XOR

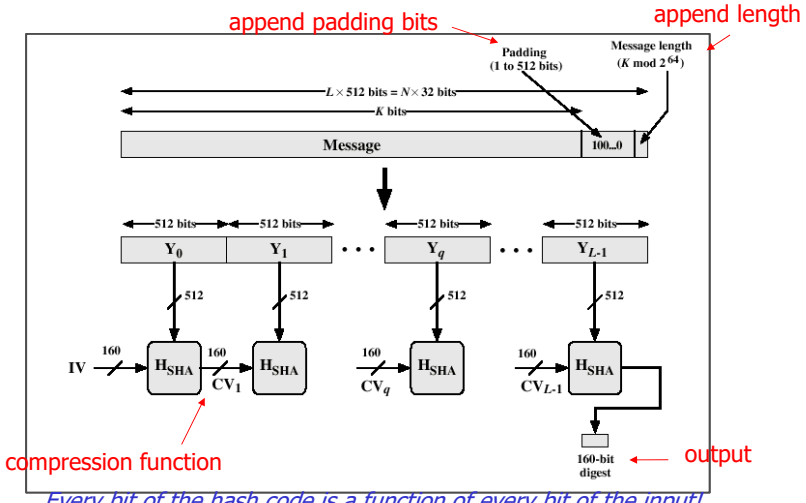
	bit 1	bit 2	• • •	bit *n*
block 1	b_{11}	b_{21}		b_{n1}
block 2	b_{12}	b_{22}		b_{n2}
	•	•	•	•
	•	•	•	•
	•	•	•	•
block *m*	b_{1m}	b_{2m}		b_{nm}
hash code	C_1	C_2		C_n

- Problema: Eliminare la predicibilità dei dati
- Randomizzazione dell'input, ottenuta con one-bit circular shift per ogni blocco

SHA-1 Secure Hash Function

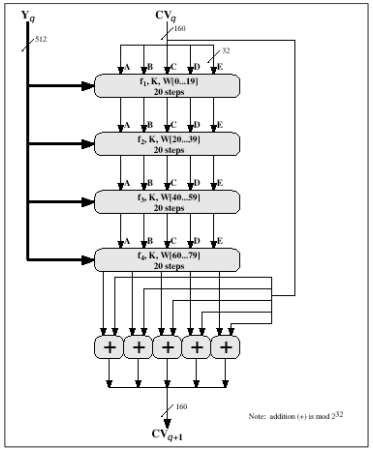
- Developed by NIST in 1995
- Input is processed in 512-bit blocks
- Produces as output a 160-bit message digest
- *Every bit of the hash code is a function of every bit of the input*
- Very secure – so far!

SHA-1 Secure Hash Function



Every bit of the hash code is a function of every bit of the input!

SHA-1 Secure Hash Function



Other Hash Functions

- Most follow basic structure of SHA-1
- This is also called an iterated hash function – Ralph Merkle 1979
- *If the compression function is collision resistant, then so is the resultant iterated hash function*
- Newer designs simply refine this structure

MD5 Message Digest

- Ron Rivest - 1992
- RFC 1321
- Input: arbitrary Output: 128-bit digest
- Most widely used secure hash algorithm – until recently
- Security of 128-bit hash code has become questionable (1996, 2004)

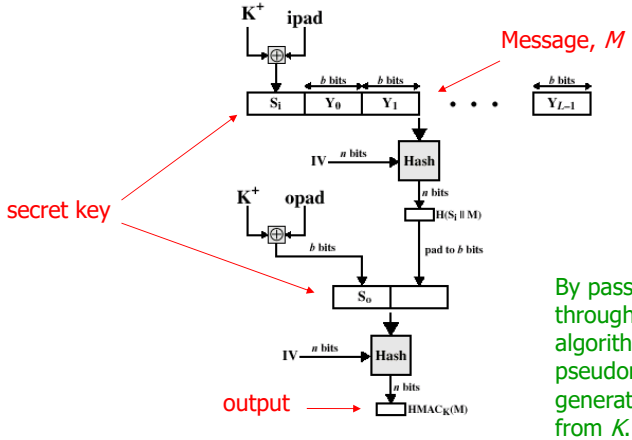
RIPEMD-160

- European RIPE Project – 1997
- Same group launched an attack on MD5
- Extended from 128 to 160-bit message digest

HMAC

- Effort to develop a MAC derived from a cryptographic hash code
- Executes faster in software
- No export restrictions
- Relies on a secret key
- RFC 2104 list design objectives
- Used in Ipsec
- Simultaneously verify integrity and authenticity

HMAC Structure



By passing S_i and S_o through the hash algorithm, we have pseudoradomly generated two keys from K.

Public Key Encryption

- Diffie and Hellman – 1976
- First revolutionary advance in cryptography in thousands of years
- Based on mathematical functions not bit manipulation
- Asymmetric, two separate keys
- Profound effect on confidentiality, key distribution and authentication

Public Key Encryption

Whitfield Diffie

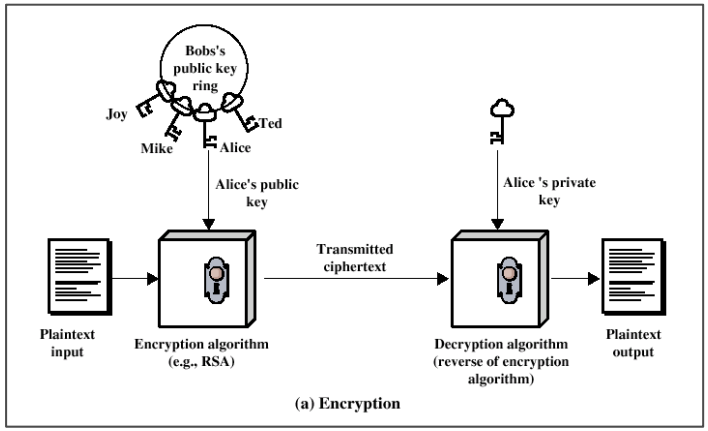
Martin Hellman

Famous Paper:
New Directions In Cryptography - 1976

Struttura della Chiave Pubblica

- Plaintext: messaggio in input all'algoritmo
- Encryption algorithm: trasformazione sul plaintext
- Public & Private Key: coppia di chiavi
  - Una per crittografare
  - Una per decrittografare
- Ciphertext: messaggio cifrato
- Decryption algorithm: produce il plaintext originale

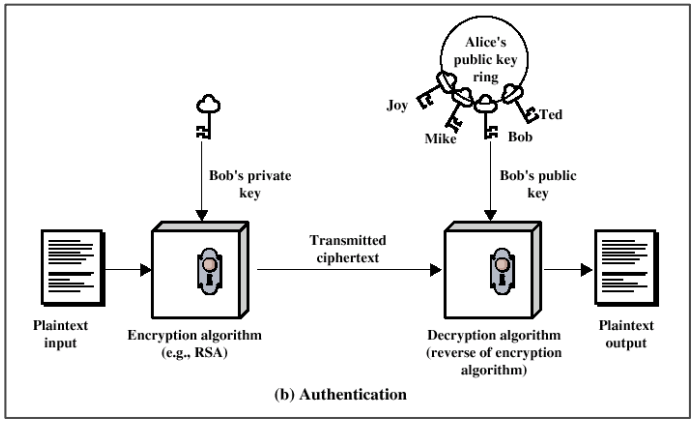
Public Key Encryption



Schema di Base

- Ogni utente genera una coppia di chiavi
  - La public key è registrata in un registro pubblico
  - La private key rimane privata
- Se Bob vuole mandare un msg privato ad Alice
  - Bob codifica il msg con la chiave pubblica di Alice
  - Quando Alice riceve il msg lo decodifica usando la sua chiave privata

Public Key Authentication



Public Key Applications

- Encryption/decryption – encrypts a message with the recipient's public key
- Digital signature – sender *signs* a message with private key
- Key Exchange – two sides cooperate to exchange a session key

Requirements For Public Key

- Easy for party B to generate pairs: public key KU_b ; private key KR_b
- Easy for sender A to generate cipertext using public key:

  $C = E_{KUb}(M)$
- Easy for receiver B to decrypt using the private key to recover original message

  $M = D_{KRb}(C) = D_{KRb}[E_{KUb}(M)]$

HINT:
PUBLIC
PRIVATE

Requirements For Public Key

- It is computationally infeasible for an opponent, knowing the public key KUb to determine the private key KR_b
- It is computationally infeasible for an opponent, knowing the public key KUb and a ciphertext, C, to recover the original message, M
- Either of the two related keys can be used for encryption, with the other used for decryption

  $M = D_{KRb}[E_{KUb}(M)] = D_{KUb}[E_{KRb}(M)]$

RSA Algorithm

- Ron Rivest, Adi Shamir, Len Adleman – 1978
- Most widely accepted and implemented approach to public key encryption
- Block cipher where M (plaintext) and C (ciphertext) are integers between 0 and $n-1$ for some n
- Following form:

  $C = M^e \bmod n$

  $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

RSA Algorithm

- Mittente e ricevente conoscono i valori di n e di e, ma solo il ricevente conosce il valore di d
- Public key: $KU = \{e,n\}$
- Private key: $KR = \{d,n\}$

RSA Requirements

- It is possible to find values of e, d, n such that $M^{ed} = M \bmod n$ for all $M<n$
- It is relatively easy to calculate M^e and C for all values of $M<n$
- It is infeasible to determine d given e and n

Here is the magic!

RSA Algorithm

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

RSA Algorithm

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

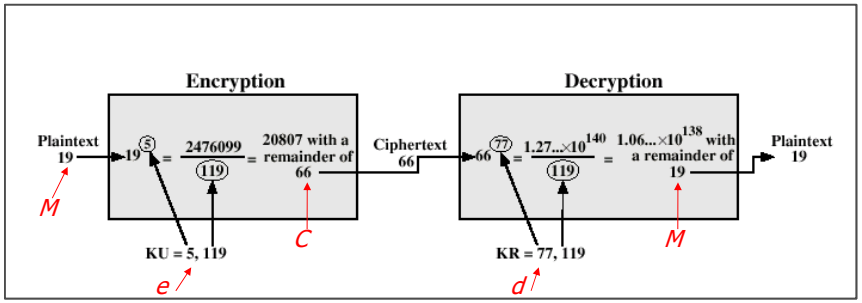
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

RSA Example

- Select two prime numbers, $p=7$ and $q=17$
- Calculate $n = pq = 7 \times 17 = 119$ ← this is the modulus
- Calculate $\phi(n) = (p-1)(q-1) = 96$ ← Euler totient
- Select e such that e is relatively prime to $\phi(n) = 96$ and less than $\phi(n)$; in this case, $e= 5$
- Determine d such that $de = 1 \bmod 96$ and $d<96$. The correct value is $d = 77$, because $77 \times 5 = 385 = 4 \times 96 + 1$

multiplicative inverse of e

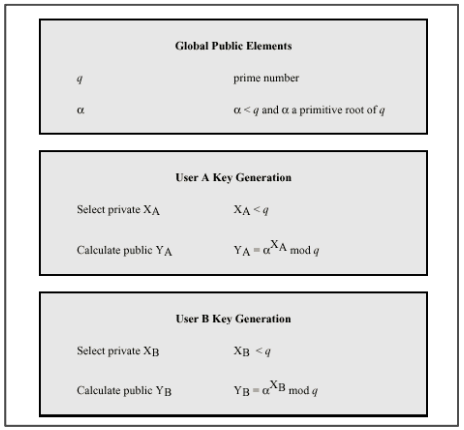
RSA Example



RSA Strength

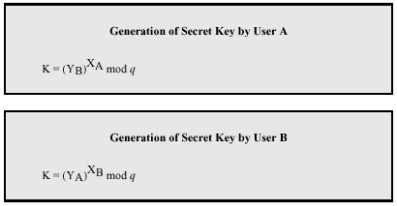
- Brute force attack: try all possible keys – the larger e and d the more secure
- The larger the key, the slower the system
- For large n with large prime factors, factoring is a hard problem
- Cracked in 1994 a 428 bit key; $100
- Currently 1024 key size is considered strong enough

Diffie-Hellman Key Exchange

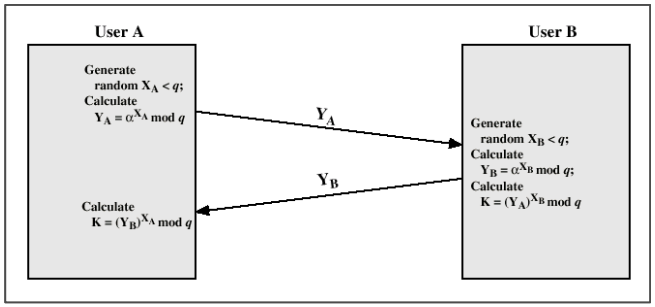


Enables two users to exchange a secret key securely.

Diffie-Hellman Key Exchange



Diffie-Hellman Key Exchange



Other Public Key Algorithms

- Digital Signature Standard (DSS) – makes use of SHA-1 and presents a new digital signature algorithm (DSA)
- Only used for digital signatures not encryption or key exchange

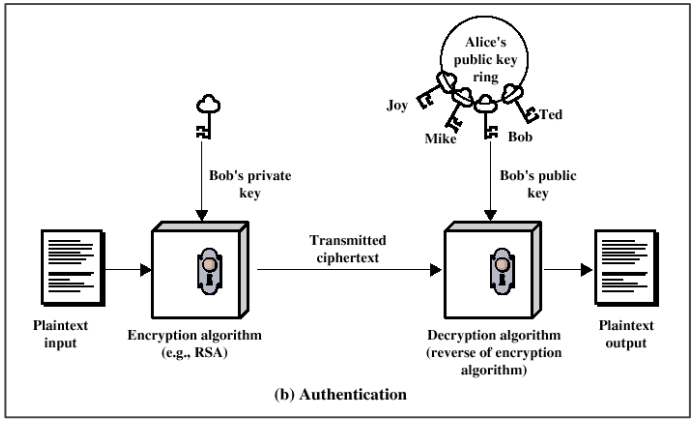
Other Public Key Algorithms

- Elliptic Curve Cryptography (ECC) – it is beginning to challenge RSA
- Equal security for a far smaller bit size
- Confidence level is not as high yet

Digital Signatures

- Use the private key to encrypt a message
- Entire encrypted message serves as a digital signature
- Encrypt a small block that is a function of the document, called an authenticator (e.g., SHA-1)

Public Key Authentication



Digital Certificate

- Certificate consists of a *public key* plus a *user ID* of the key owner, with the whole block signed by a trusted third party, the certificate authority (CA)
- X.509 standard
- SSL, SET and S/MIME
- Verisign is primary vendor

Public Key Certificate Use