Cryptography

(the art of scrambling)

1

Beside programming e-commerce applications, what other cs issues are there?

- Application (web) design: HCI
- Data mining
- Server and client security (how can we protect our systems and data
  - hackers
  - malicious code
  - denial-of-service (DOS) attacks
  - privacy
- Electronic document authentication

2

Major issues

- Secret message
  - Write a message that only your friend can read while passing it through enemy lines
- Message authentication

Dear Jean,

I love you

George

This is $1000 Dollar (US!!)

more formally …

1. Confidentiality:
   - how can I make sure that an eavesdropper can not read my message
2. Authentication:
   - how do I know that the message is from a particular person?
3. Message integrity:
   - how do I know that the message has not been modified on its travel?

Basic Cryptography

(Outline)

- Ciphers
- Symmetric Key Algorithms (1. Confidentiality)
- Public Key Algorithms (2. Authentication)
- Message Digests (3. Message integrity)
- Digital Signatures
- Trust networks

5

1. Confidentiality

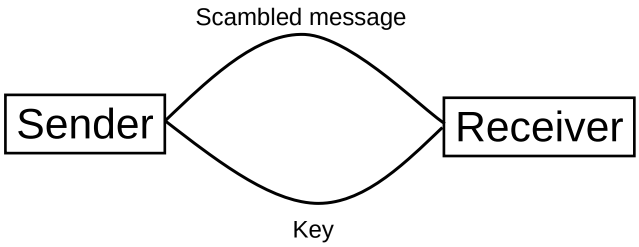
Top Secret

6

Encryption-Decryption

- Main idea: scramble a message so that it is impossible (or very difficult) to read the message unless I tell you another secret that makes it possible to de-scramble it.

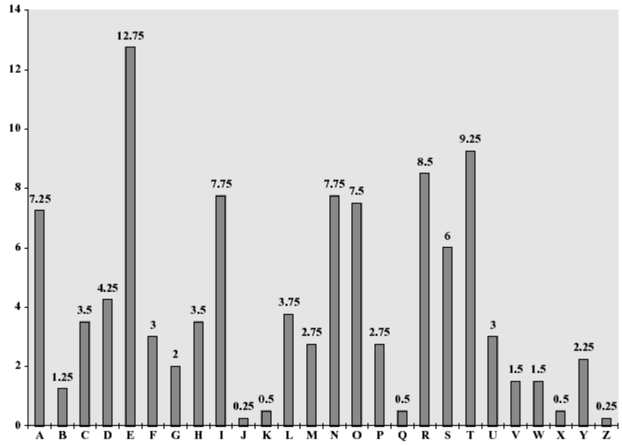
- Two route solution to privacy:



- Key could be
  - Secret scambling procedure (not good)
  - Secret input to scrambling procedure (good)


```
guvf zrffntr vf frperg
___s __ss___ _s s_____
__is __ss___ is s_____
```

Relative frequency of letters in English text



9

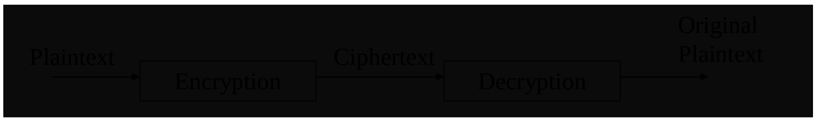
```
guvf zrffntr vf frperg
___s __ss___ _s s_____
__is __ss___ is s_____
__is _ess__e is se__e_
this _ess__e is se__et
this message is secret
```

ROT13 algorithm (cipher):

```
abcdefghijklmnopqrstuvwxyz
          ↓
nopqrstuvwxyzabcdefghijklm
```

10

Definitions
(Encryption, Decryption, Plaintext, Ciphertext)

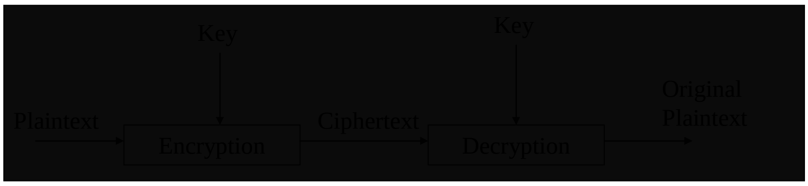


Types of cipher:

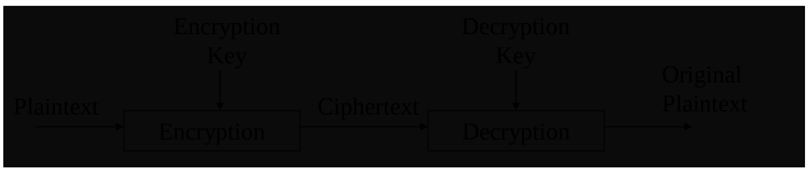
- Stream cipher
  - Each bit (or byte) is encrypted or decrypted individually
  - Simple substitution ciphers (ROT13, XOR)
- Block cipher
  - A sequence of bits (or bytes) is used at each step in the encryption and decryption process (DES, AES)

11

Symmetric Key Algorithms



Public Key Cryptography



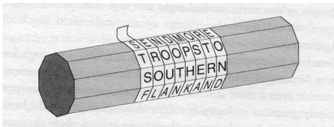
12

Symmetric Key Algorithms

General:

- Substitution (ROT13, Cryptoquotes)
- Transposition
- XOR
- One Time Pad

} most practical algorithms use a combination of these



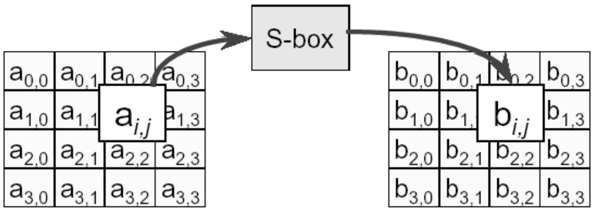
Specific algorithms:

- DES (data encryption standard, 56-bit key , Triple-DES)
- IDEA (international data encryption algorithm, 128-bit key, patents)
- RC2, RC4, RC5 (Ronald Rivest RSA, variable key length)
- **Rijndael (AES) (advanced encryption standard adapted in 2001)**

Rijndael: Iterated Block Cipher

- 10/12/14 times applying the same round function
- Round function: uniform and parallel, composed of 4 steps
- Each step has its own particular function:
  1. ByteSub: nonlinearity
  2. ShiftRow: inter-column diffusion
  3. MixColumn: inter-byte diffusion within columns
  4. Round key addition

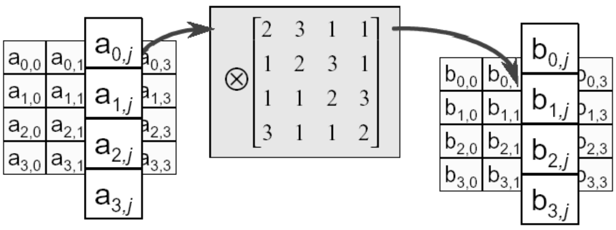
Round step 1: ByteSub



- Bytes are transformed by applying invertible S-box.
- One single S-box for the complete cipher
- <u>High non-linearity</u>

15

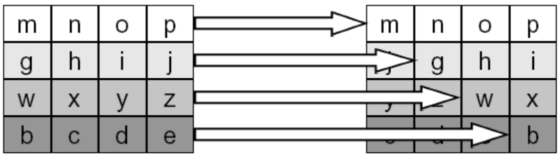
Round step 2: MixColumn



- Bytes in columns are linearly combined
- Based on theory of error-correcting codes
- <u>High intra-column diffusion</u>

16

Round step 3: ShiftRow



- Rows are shifted over 4 different offsets
- Interaction with MixColumn
- High diffusion over multiple rounds

17

Round step 4: Key addition

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} + \begin{bmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{bmatrix} = \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{bmatrix}$$

- Makes round function key-dependent
- Computation of round keys: “keep it simple”
- Small number of operations
- Small amount of memory

18

What is an appropriate length for a key?

Table 3-1. Estimated success of brute force attacks (for different numbers of bits in the key and number of keys that can be tried per second)

Length of key	Keys searched per second	Postulated key searching technology[a]	Approximate time to search all possible keys
40 bits[b]	10	10-year-old desktop computer	3,484 years
40 bits	1,000	Typical desktop computer today	35 years
40 bits	1 million	Small network of desktops	13 days
40 bits	1 billion	Medium-sized corporate network	18 minutes
56 bits	1 million	Desktop computer a few years from now	2,283 years
56 bits	1 billion	Medium-sized corporate network	2.3 years
56 bits[c]	100 billion	DES-cracking machine	8 days
64 bits	1 billion	Medium-sized corporate network	585 years
80 bits	1 million	Small network of desktops	38 billion years
80 bits	1 billion	Medium-sized corporate network	38 million years
128 bits	1 billion	Medium-sized corporate network	10^{22} years
128 bits	1 billion billion (1×10^{18})	Large-scale Internet project in the year 2005	10,783 billion years
128 bits	1×10^{23}	Special-purpose quantum computer, year 2015?	108 million years
192 bits	1 billion	Medium-sized corporate network	2×10^{41} years
192 bits	1 billion billion	Large-scale Internet project in the year 2005	2×10^{32} years
192 bits	1×10^{23}	Special-purpose quantum computer, year 2015?	2×10^{27} years
256 bits	1×10^{23}	Special-purpose quantum computer, year 2015?	3.7×10^{46} years
256 bits	1×10^{32}	Special-purpose quantum computer, year 2040?	3.7×10^{37} years

[a] Computing speeds assume that a typical desktop computer in the year 2001 can execute approximately 500 million instructions per second. This is roughly the speed of a 500 Mhz Pentium III computer.
[b] In 1997, a 40-bit key was cracked in only 3.5 hours.
[c] In 2000, a 56-bit key was cracked in less than 4 days.

Comparison of cryptographic algorithms

a bit old

Table 3-2. Common symmetric encryption algorithms

Algorithm	Description	Key Length	Rating
Blowfish	Block cipher developed by Schneier	1–448 bits	Λ
DES	Data Encryption Standard adopted as a U.S. government standard in 1977	56 bits	§
IDEA	Block cipher developed by Massey and Xuejia	128 bits	Λ
MARS	AES finalist developed by IBM	128–256 bits	ø
RC2	Block cipher developed by Rivest	1–2048 bits	Ω
RC4	Stream cipher developed by Rivest	1–2048 bits	Λ
RC5	Block cipher developed by Ronald Rivest and published in 1994	128–256 bits	ø
RC6	AES finalist developed by RSA Labs	128–256 bits	ø
Rijndael	NIST selection for AES, developed by Daemen and Rijmen	128–256 bits	Ω
Serpent	AES finalist developed by Anderson, Biham, and Knudsen	128–256 bits	ø
Triple-DES	A three-fold application of the DES algorithm	168 bits	Λ
Twofish	AES candidate developed by Schneier	128–256 bits	ø

Key to ratings:

Ω) Excellent algorithm. This algorithm is widely used and is believed to be secure, provided that keys of sufficient length are used.

Λ) Algorithm appears strong but is being phased out for other algorithms that are faster or thought to be more secure.

ø) Algorithm appears to be strong but will not be widely deployed because it was not chosen as the AES standard.

§) Use of this algorithm is no longer recommended because of short key length or mathematical weaknesses. Data encrypted with this algorithm should be reasonably secure from casual browsing, but would not withstand a determined attack by a moderately-funded attacker.

2. Authentication

It's me ....

.... really!

Key distribution problem

- How to ship the 'code-book'?
- Solutions
  - Doubly padlocked box exchange
  - Diffie-Hellman key exchange
  - Public-key cryptography
    - RSA
    - elliptic curve cryptography

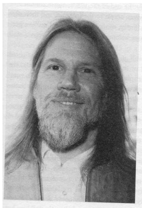


Figure 62 Whitfield Diffie.

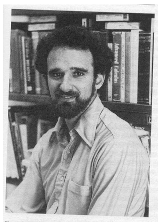
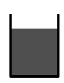
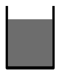
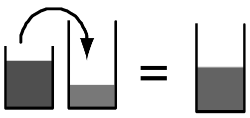
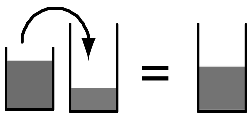
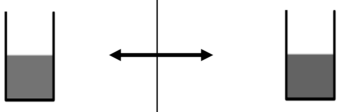
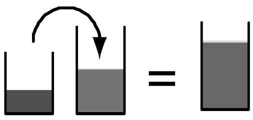
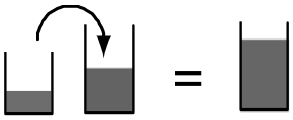


Figure 63 Martin Hellman.

Figure 65 Ronald Rivest, Adi Shamir and Leonard Adleman.

Diffie-Hellman key exchange (1)

	Alice	Bob
Secret part generation		
One-way function		
Swap		
Key generation		

Diffie-Hellman key exchange (2)

	Alice	Bob
Secret part generation	Choose a secret number A=3	Choose a secret number B=6
One-way function	Use one-way function $a=7^A \pmod{11}=2$	Use one-way function $b=7^B \pmod{11}=4$
Swap	b=4	a=2
Key generation	Another one-way function $k=b^A \pmod{11}=9$	Another one-way function $k=a^B \pmod{11}=9$

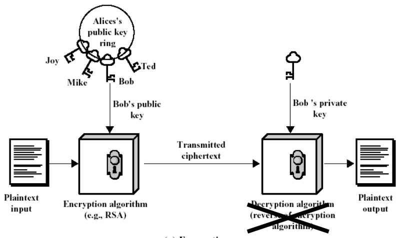
Diffie-Hellman key exchange (3)

- The Diffie-Hellman key exchange was the first widely recognized
- Solution to the key exchange problem
- Can only be used to exchange key. Symmetric key cryptographic methods can be used to exchange secret messages
- Fairly elaborate exchange of messages

25

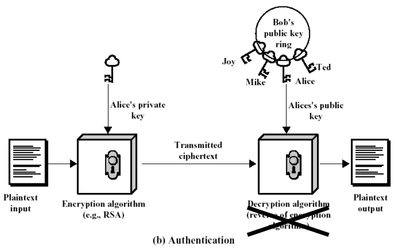
Public Key Cryptography

- A public key - private key pair are used, one for encryption and the other for decryption



(a) Encryption

- Two application modes:
  - Confidentiality
  - Authentication



(b) Authentication

26

Public Key Cryptography a la RSA

<u>Public Key:</u>
n - product of two primes, *p* and *q* (*p* and *q* are secret)
e - relatively prime to $(p-1)(q-1)$ (have no common divisor)

<u>Private Key:</u>
d - $e^{-1} \bmod ((p-1)(q-1))$

<u>Encrypting:</u>
$c = m^e \bmod n$

<u>Decrypting:</u>
$m = c^d \bmod n$

Example:

- Let p=3, q=11
- $n=pq$=33
- e must be relatively prime to $(p-1)(q-1)$=20
- choose e = 7, then $d = 7^{-1} \bmod 20 = 3$
- Plaintext is 3,4,2 (m_1=3, m_2=4, m_3=2)
- $c_1=m_1^e \bmod n = 3^7 \bmod 33 = 9$
- $c2 = m2^e \bmod n = 4^7 \bmod 33 = 15$
- $c3 = m3^e \bmod n = 2^7 \bmod 33 = 29$
- Ciphertext is 9,15,29
- $m_1=c_1^d \bmod n = 9^3 \bmod 33 = 3$
- $m_2=c_2^d \bmod n = 15^3 \bmod 33 = 4$
- $m_3=c_3^d \bmod n = 29^3 \bmod 33 = 2$
- Plaintext is 3,4,2

27

3. Message Integrity

28

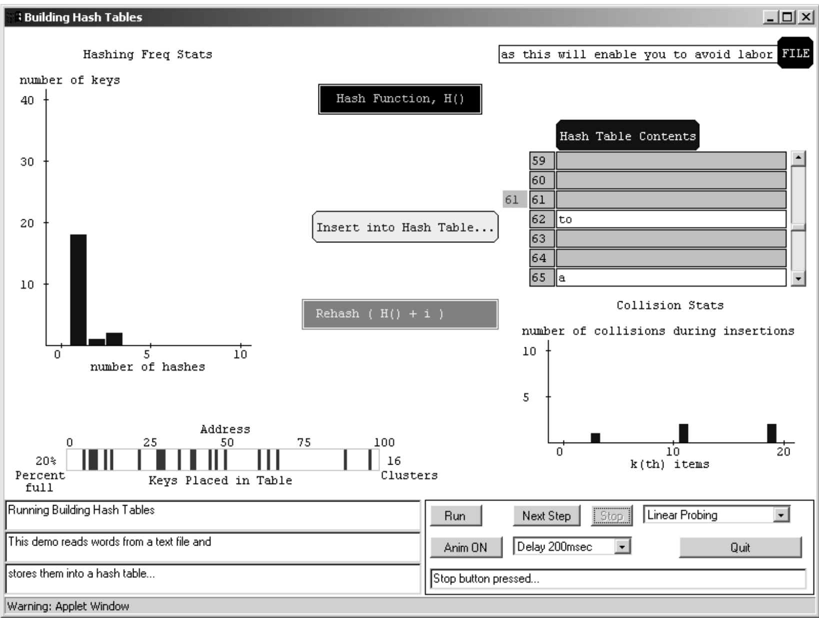
Message Digests & Hash function

- A message digest is a one-way function which maps the information contained in a (small or large) file to a single large number, typically between 128 bits and 256 bits in length.

- A good message digest function should have the following properties:
  - Every bit of the output is influenced by every bit of the input
  - Changing a single bit in the input results in every output bit having a 50% chance of changing
  - Given an input file, its corresponding digest, and the digest function, it is computationally infeasible to produce another input file which maps to the same digest

29

http://ciips.ee.uwa.edu.au/~morris/Year2/PLDS210/hash_tables.html

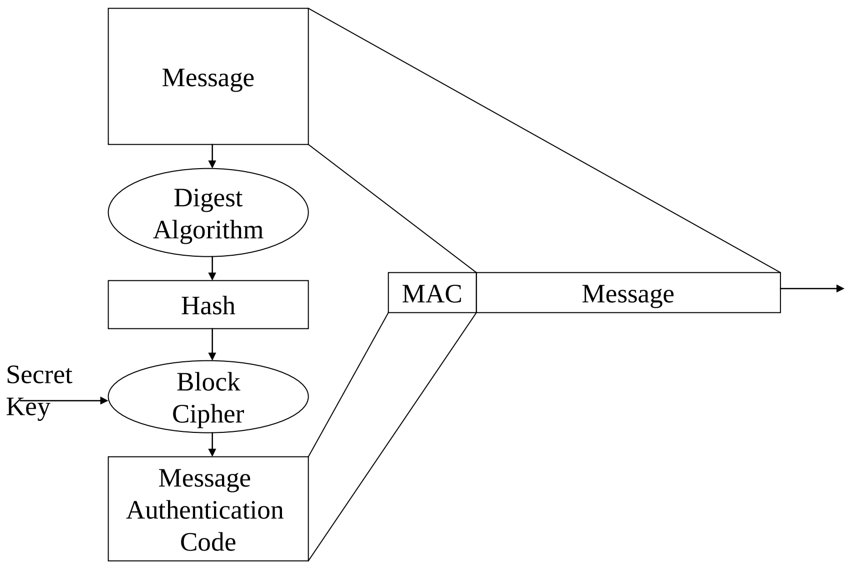


Message Digests (continued)

- Standard encryption algorithm
  - e.g. use last block in cipher feedback mode
  - Provide good message digest code
  - Computationally more demanding than other specialized functions
- MD5
  - One widely used message digest algorithm from a series of algorithms developed by Ronald Rivest
  - Does not rely on a secrete key and is therefore not suitable as MAC without further provisions
- HMAC
  - The Hashed Message Authentication Code uses a shared secret key in combination with a message digest function to produce a secret message authentication code
  - Since an attacker doesn't know the secret, the attacker cannot produce a correct authentication code if they alter the message
  - Fast to calculate, can be used as digital signature. However, a shared secret key is used.
- SHA-1
  - Developed by the NSA for use with the Digital Signature Standard

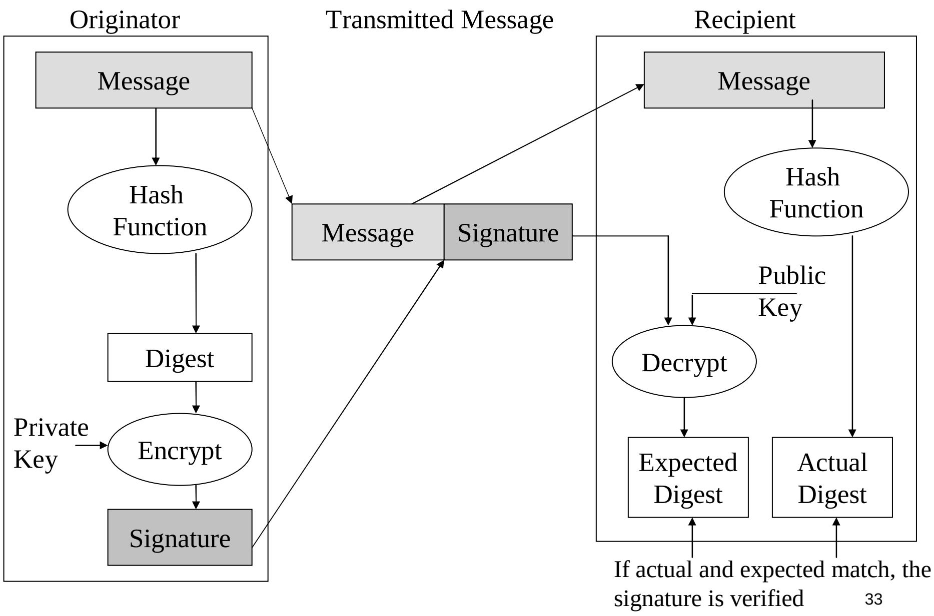
31

Operation of a message digest function to produce a message authentication code



32

RSA Digital Signature



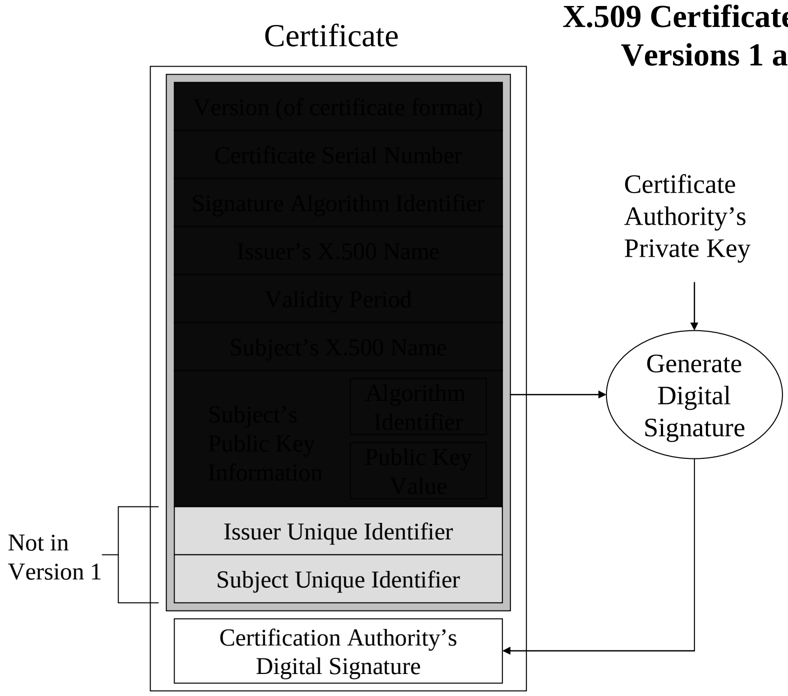
Types of authentication

- What you know (username and password)
- What you have (token, smart card)
- What you are (biometrics)
- Where you are (location security)

Digital Certificates

- Need a system for pairing public keys to identification information
- Certification authority (or *trusted third party*) issues a certificate which pairs identification information with a public key, signed with the certification authority's private key
- User must trust the certification authority, and have a valid copy of the certification authority's public key

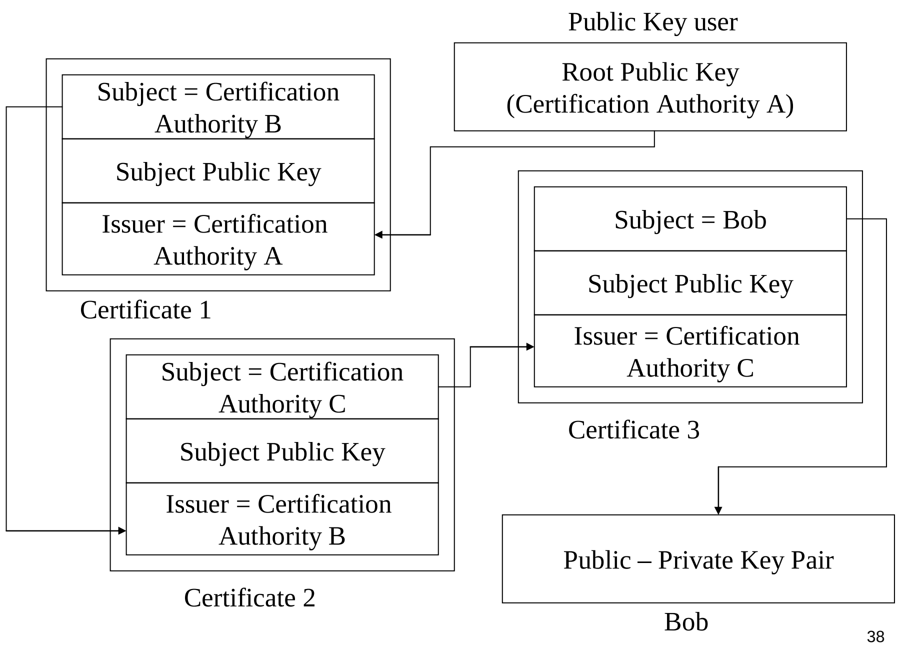
X.509 Certificate Format Versions 1 and 2



Certification Paths

- More than one Certification Authority will be required
- If CAs trust one another, they can issue certificates for each other’s public keys
- This leads to a recursively defined path from a user under one CA to a user under another CA

37



38

Blind Signatures

- Analogy – place a document to be signed inside an envelope with a carbon paper over it, and have the signing party sign the envelope. Signing the envelope causes the document to be signed because of the carbon paper inside.

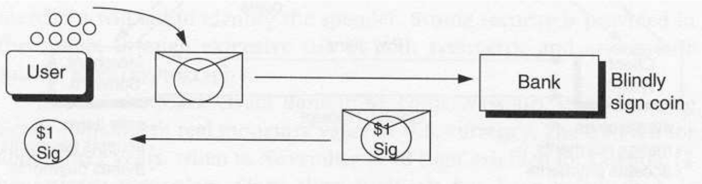


Figure 6.2 Blind signature analogy for withdrawing Ecash coins.

PGP: Pretty Good Privacy

Philip Zimmermann

PGP
CORPORATION

• Implementation of best available cryptographic algorithms for confidentiality and authentication and integration into a freely available general-purpose application

• Package, source code, and documentation available on the web

•Low-cost commercial version initially from Network Associates (now from PGP Corporation)

•Includes AES, 3DES, CAST, IDEA; RSA DSS, Diffie-Hellman; SHA1; key management, …