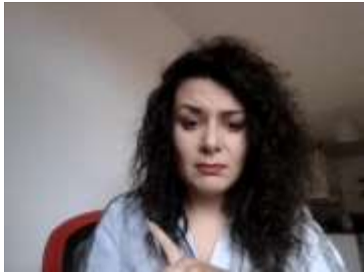
Computer System- B Security

Introduction to Cryptography

Alma
Oracevic

Agenda

- A non-technical brief introduction to cryptography
- Where/how/why they are used in practice (real examples to follow)
- You will have more rigorous treatment in other units



Security services

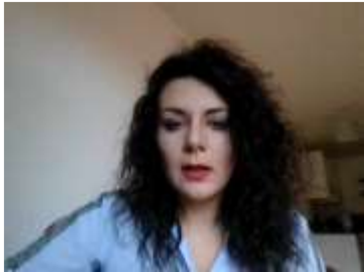
Protecting data

in transit

- **confidentiality**
- **integrity**
- **authentication**
- **non-repudiation**

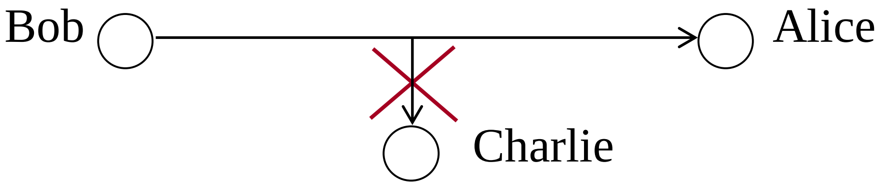
at rest

- **access control**
  - **identification**
  - **authorization**
  - **auditing**
- **availability**

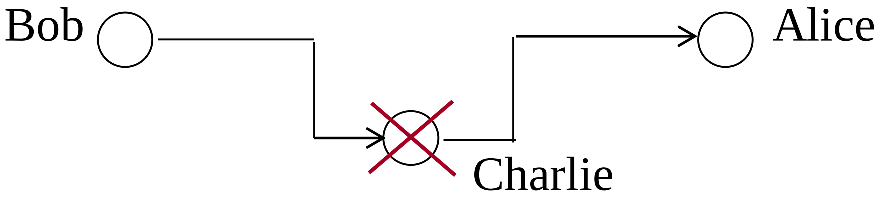


Basic Security Services (1)

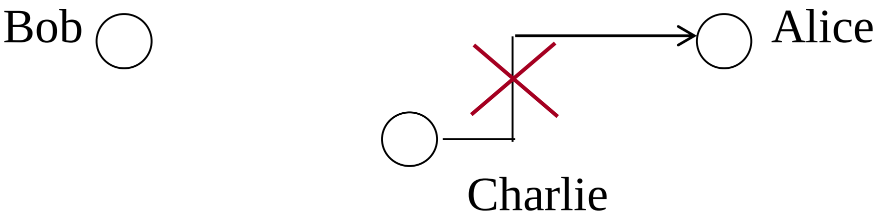
1. Confidentiality

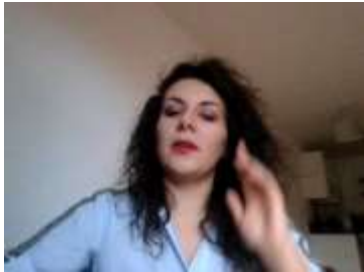


2. Message integrity



3. Message authentication





Basic Security Services (2)

4. Non-repudiation

- of sender - of receiver - mutual

Technique: *digital signature*

Signature

DIGITAL

HANDWRITTEN

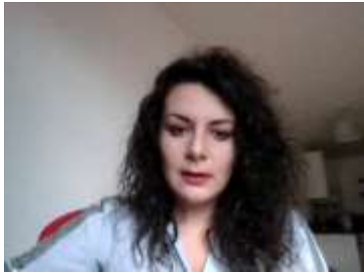
A6E3891F2939E38C745B
25289896CA345BEF5349
245CBA653448E349EA47

Main Goals:
- unique identification
- proof of agreement to the contents of the document

User Authentication

On the basis of

- **what you know** (passwords, PINs)
- **what you have** (magnetic card, smart card)
- **what you are** (fingerprints, handprints, voiceprints, keystroke timing, signatures, retinal scanners)

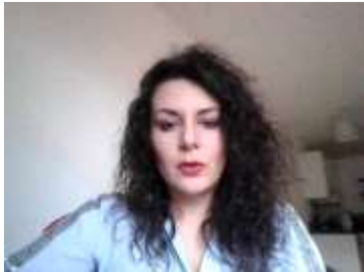


What is encryption

Encryption?

Encryption is the process of encoding information.

This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.

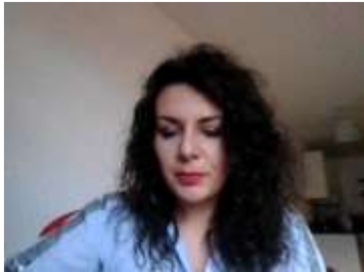



HEART
ALICE !
I LOVE YOU
BOB
1995.05.10 12:05
IBM
PC


HEART
ALICE
I LOVE YOU
BOB
1995.05.10 12:05
IBM
PC

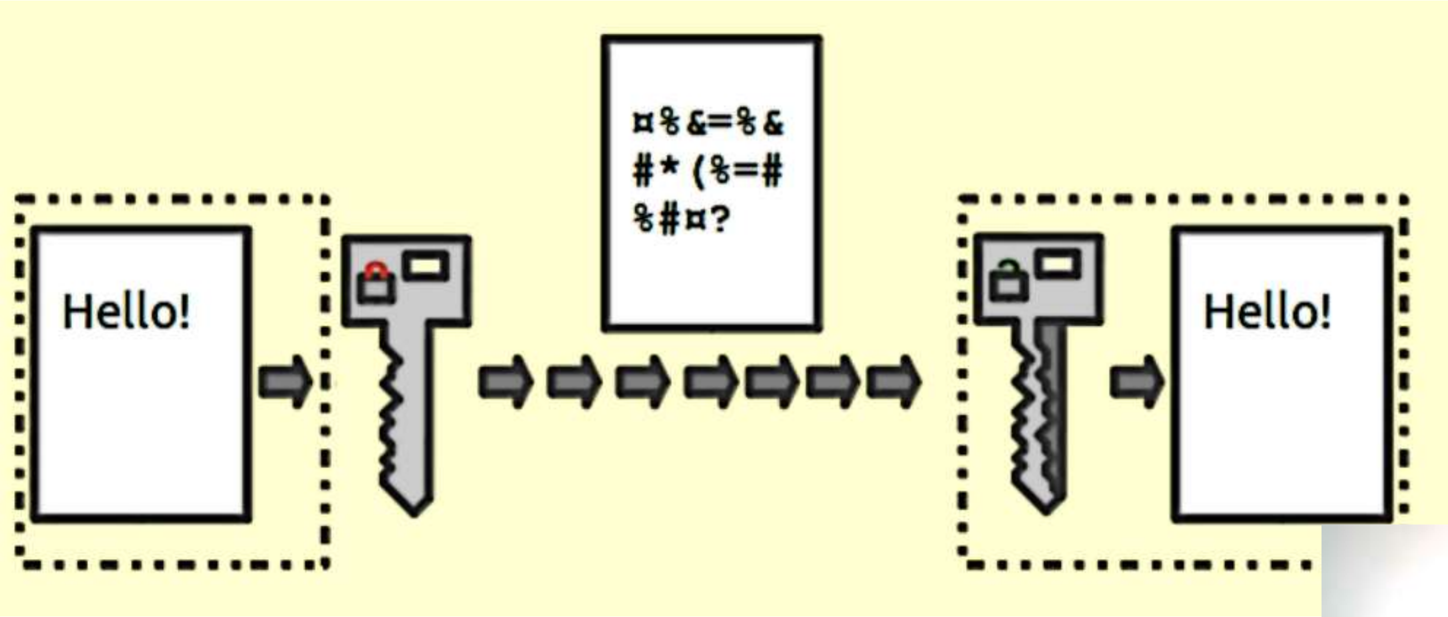


TITAN



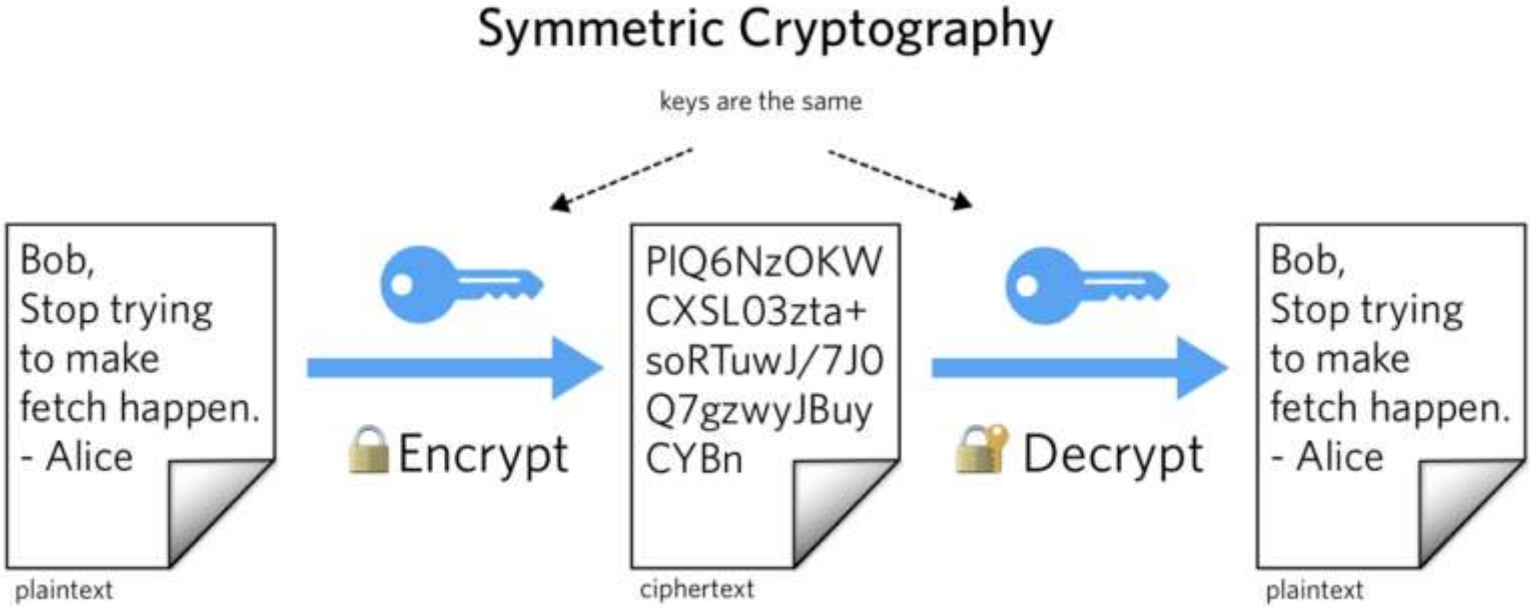
Is it something new?

How does it work?



Applications?

How does Symmetric encryption work?



Essential elements

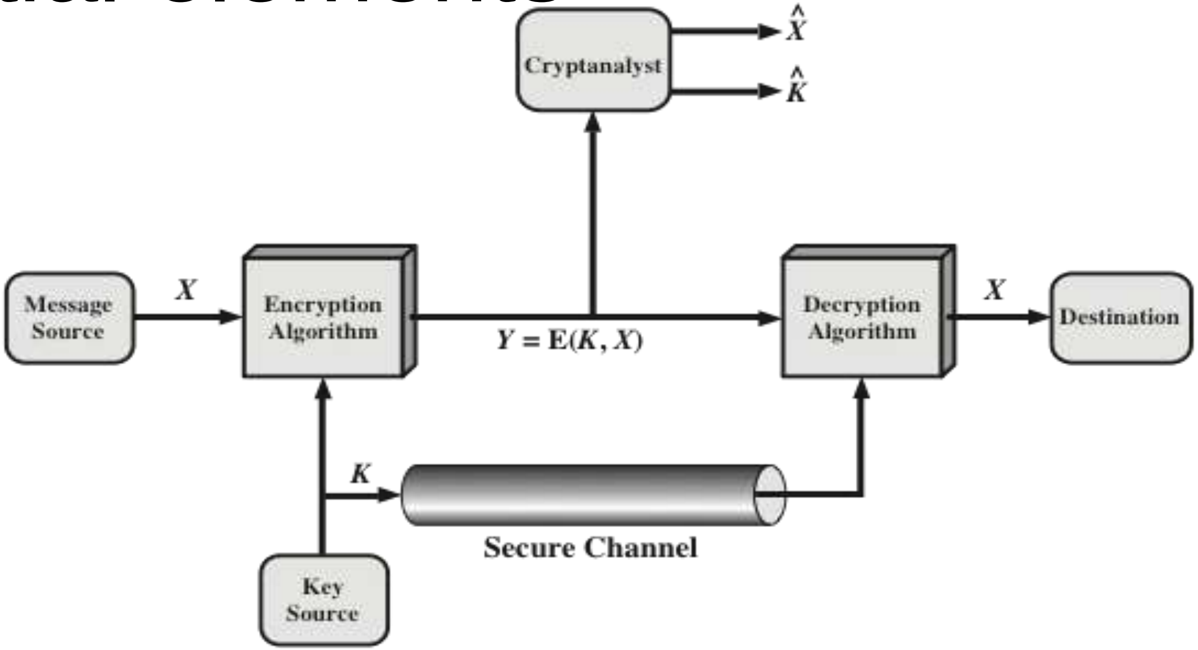
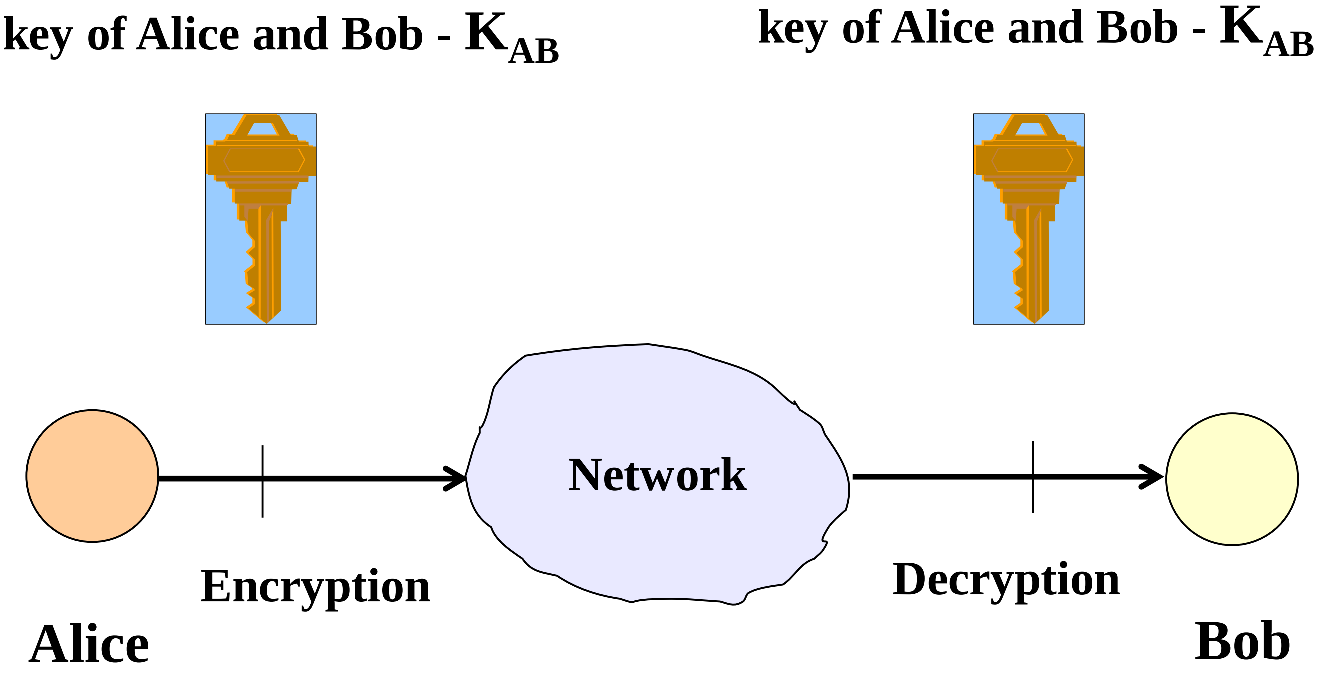


Figure 3.2 Model of Symmetric Cryptosystem

Cryptography and Network Security, Seventh Edition by William Stallings

Secret-key (Symmetric) Cryptosystems

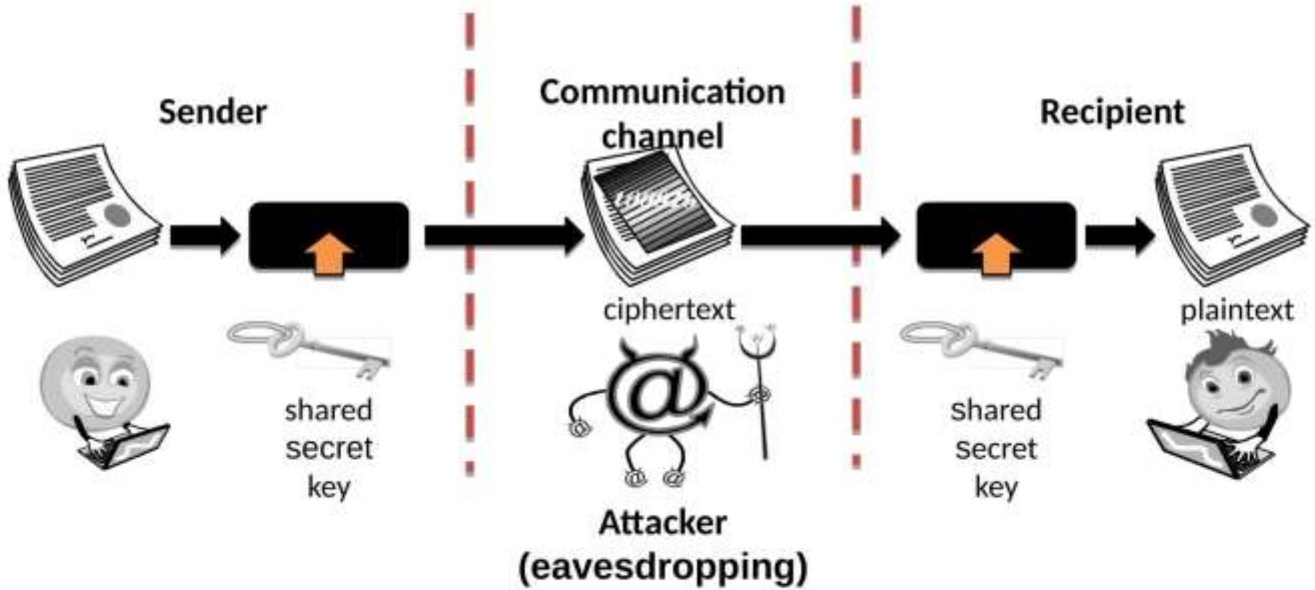


Symmetric Cryptosystems

- Alice and Bob share a secret key, which is used for both encryption and decryption.

Symmetric Cryptosystems

- Alice and Bob share a secret key, which is used for both encryption and decryption.



Symmetric Key Distribution

- Requires each pair of communicating parties to share a (separate) secret key.

Symmetric Key Distribution

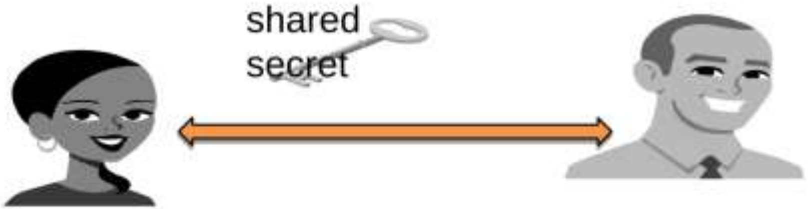
- Requires each pair of communicating parties to share a (separate) secret key.

Symmetric Key Distribution

- Requires each pair of communicating parties to share a (separate) secret key.

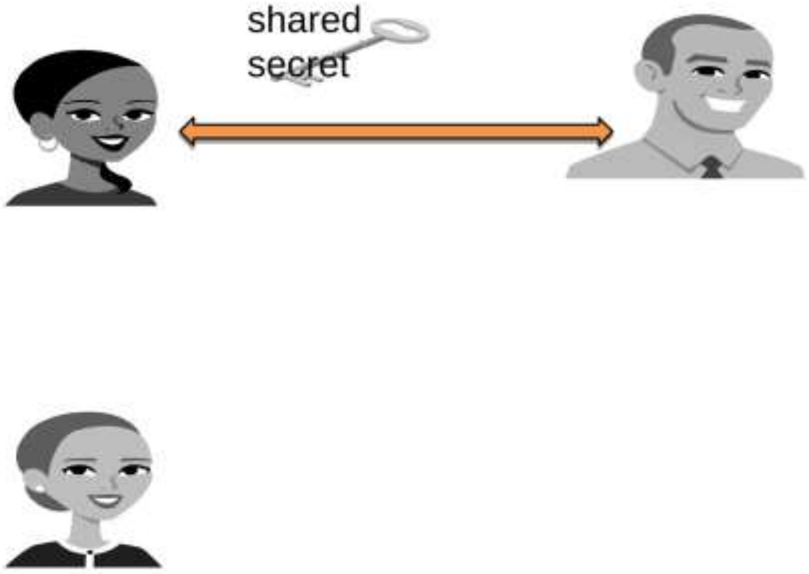
Symmetric Key Distribution

- Requires each pair of communicating parties to share a (separate) secret key.



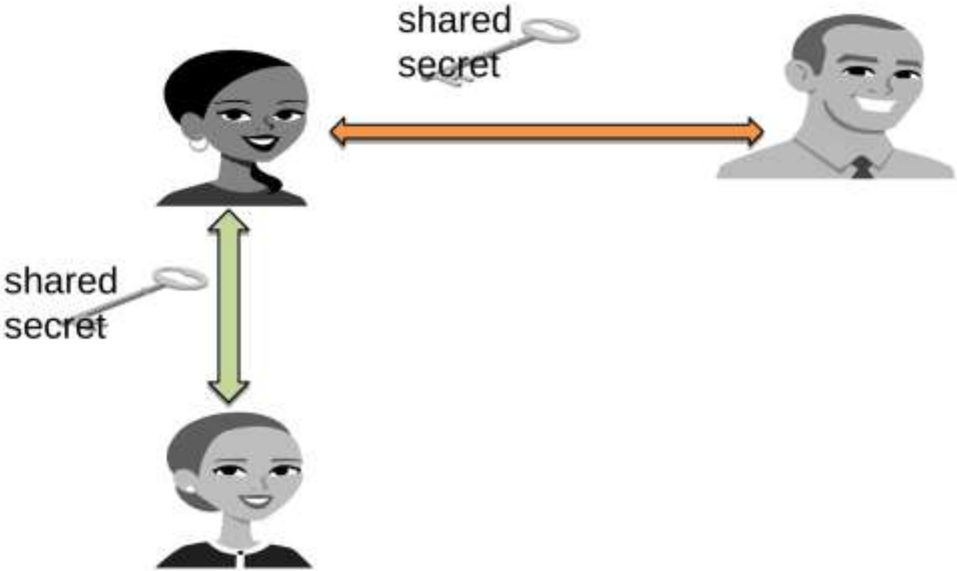
Symmetric Key Distribution

- Requires each pair of communicating parties to share a (separate) secret key.



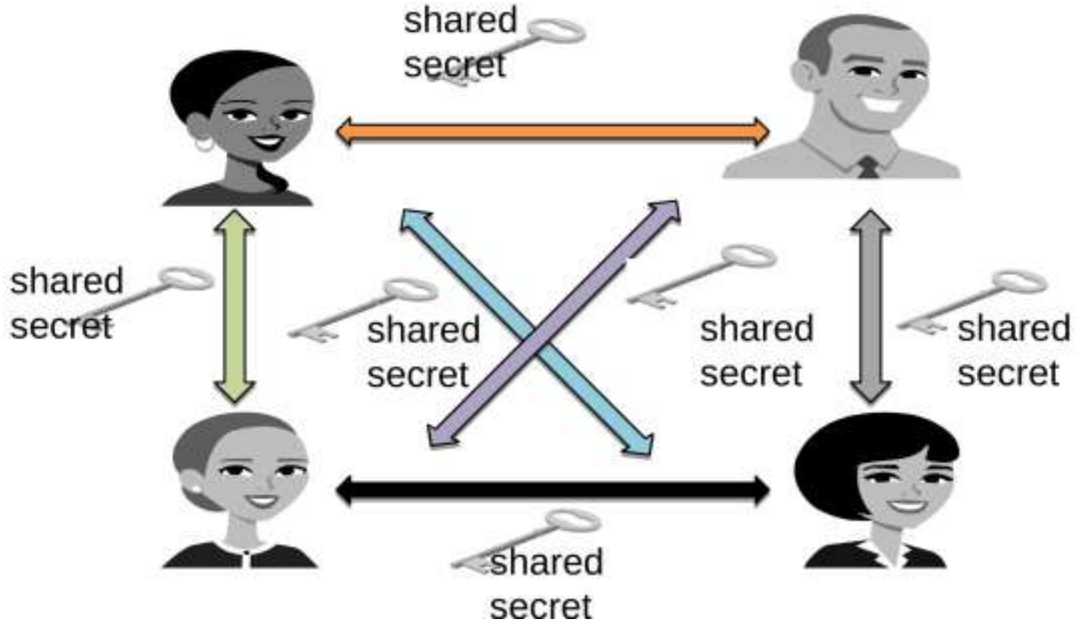
Symmetric Key Distribution

- Requires each pair of communicating parties to share a (separate) secret key.



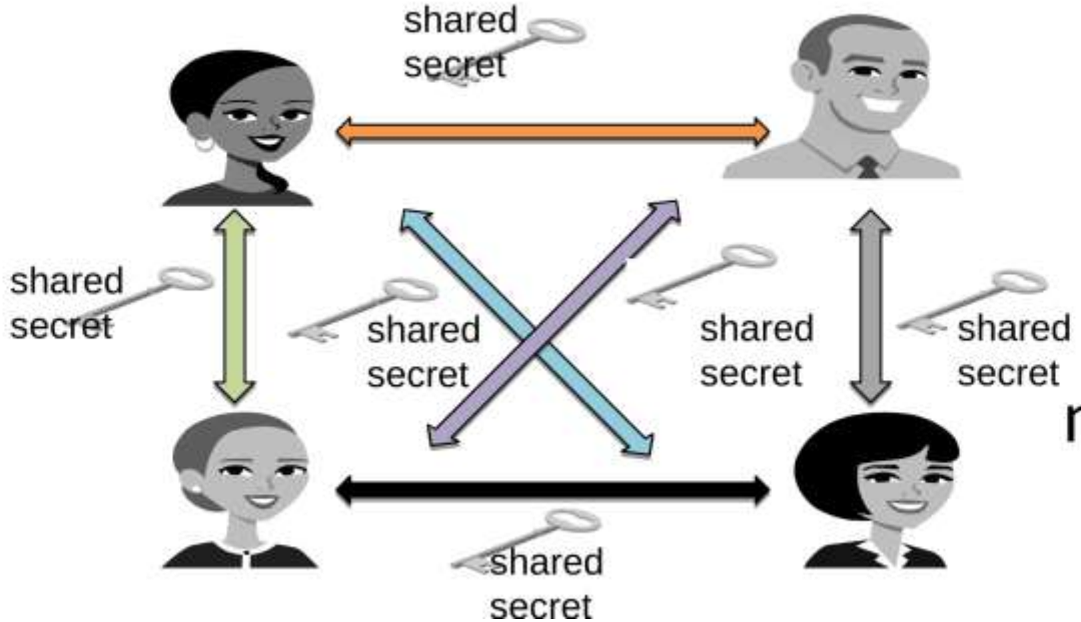
Symmetric Key Distribution

- Requires each pair of communicating parties to share a (separate) secret key.



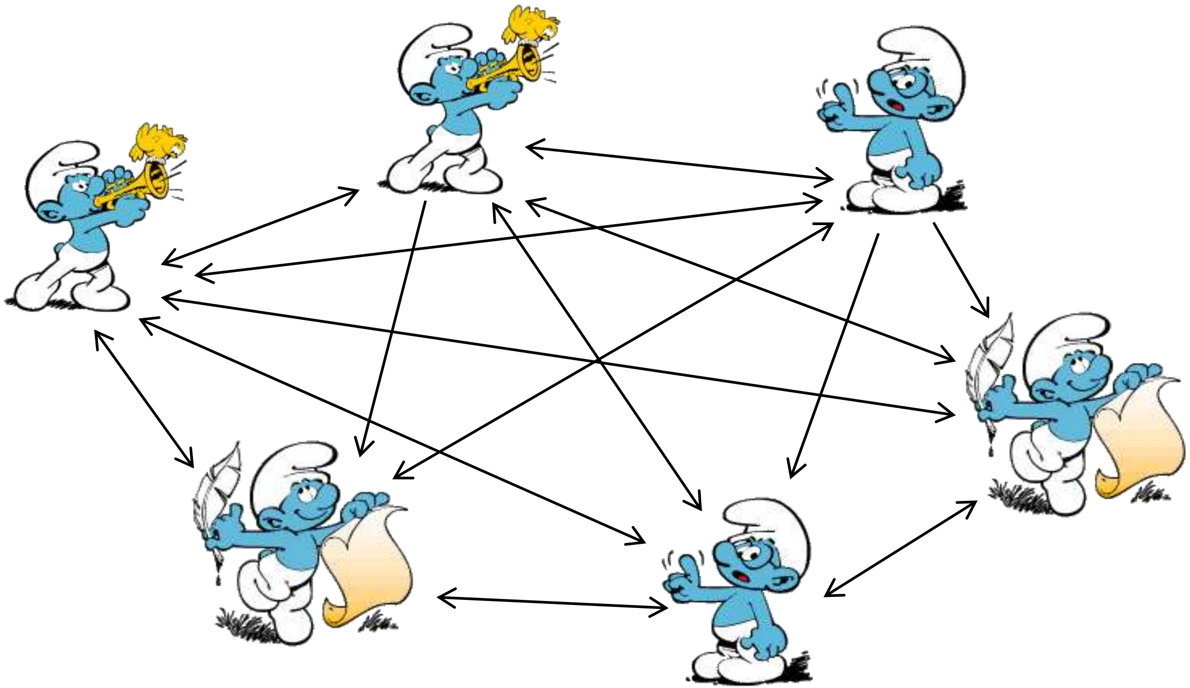
Symmetric Key Distribution

- Requires each pair of communicating parties to share a (separate) secret key.



n (n-1)/2 keys

Key Distribution Problem



N - Users $\Rightarrow$ $\dfrac{N \cdot (N-1)}{2}$ Keys

Users	Keys
100	5,000
1000	500,000

Symmetric Key conti...

- Data Encryption Standard- DES (triple DES)
- Computationally scalable for large messages
- Hardware implementation is available.

- Advanced Encryption Standard -AES (current standard)

  key lengths: 128, 192 and 256 bits

  – AES-NI (intel)

- Key distribution is a challenge!

Public-Key Cryptography

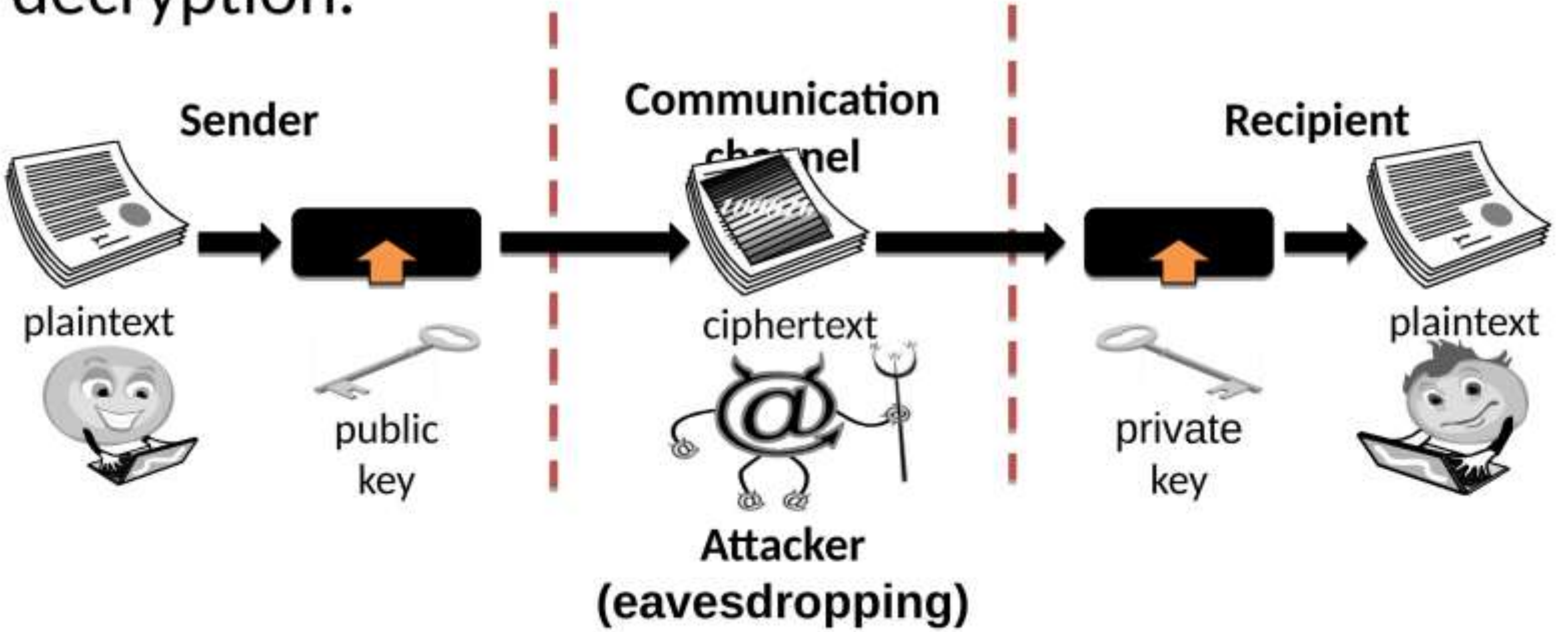
- Bob has two keys: a **private key**, SB, which Bob keeps secret, and a **public key**, PB, which Bob broadcasts widely.
  - In order for Alice to send an encrypted message to Bob, she need only obtain his public key, PB, use that to encrypt her message, M, and send the result, $C = E_{PB}(M)$, to Bob. Bob then uses his secret key to decrypt the message as $M = D_{SB}(C)$.

Public-Key Cryptography

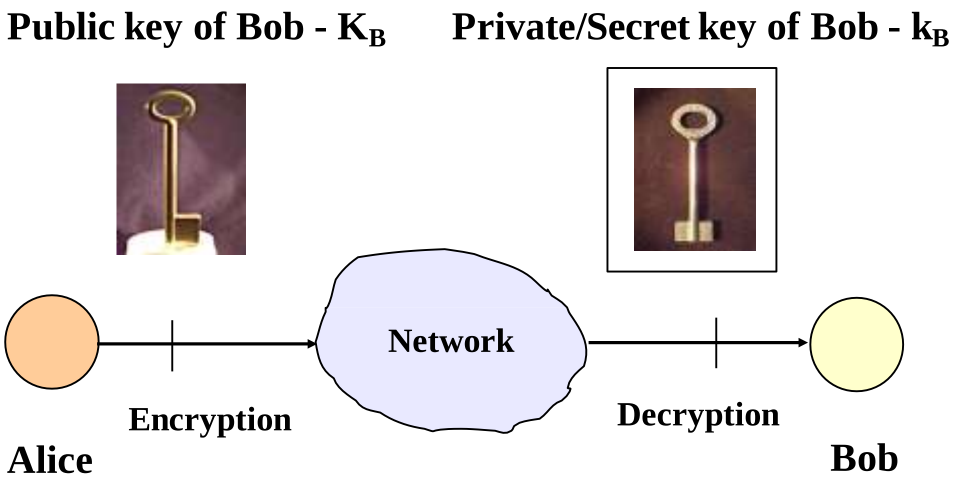
- Separate keys are used for encryption and decryption.

Public-Key Cryptography

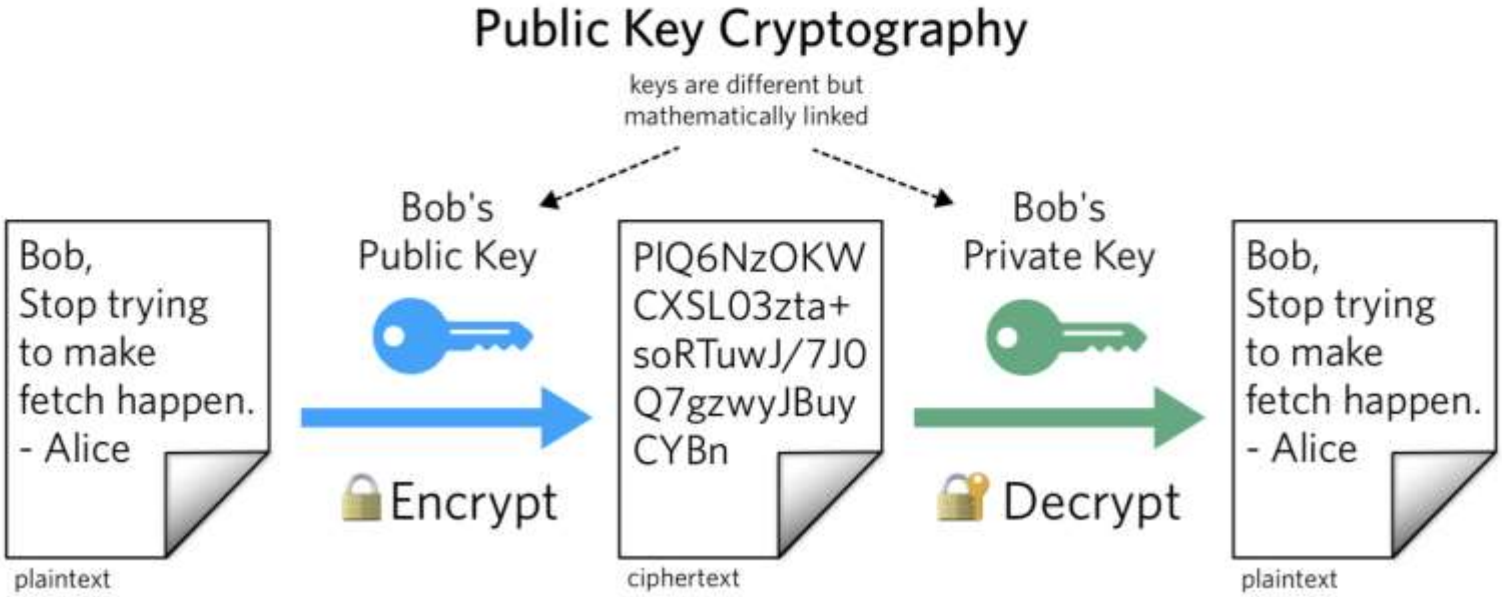
- Separate keys are used for encryption and decryption.



Public Key (Asymmetric) Cryptosystems



How does Asymmetric encryption work?

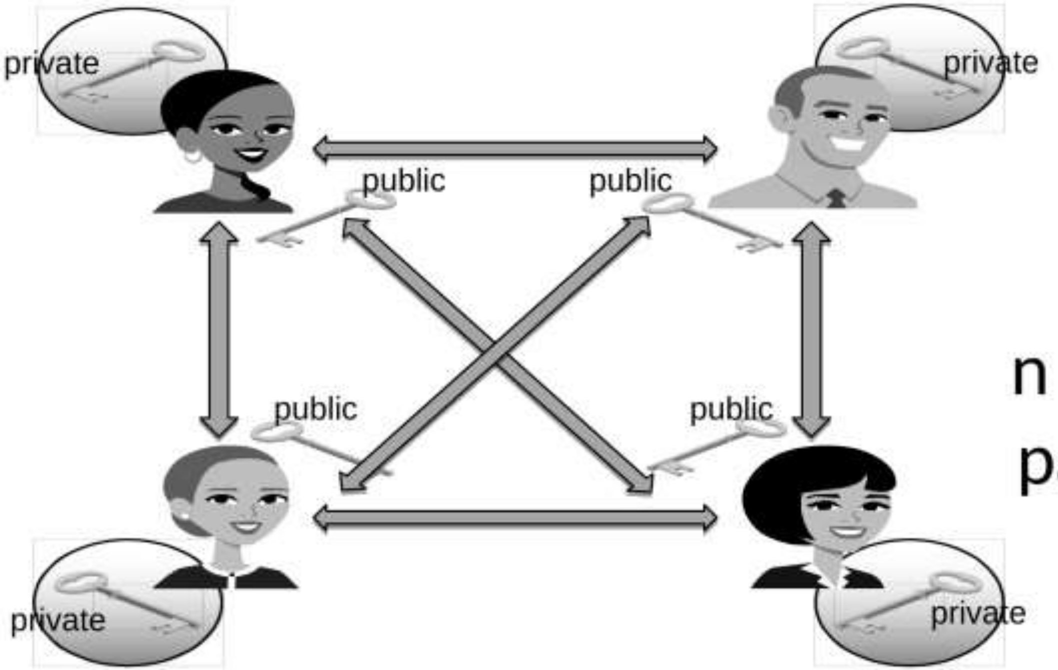


Public Key Distribution

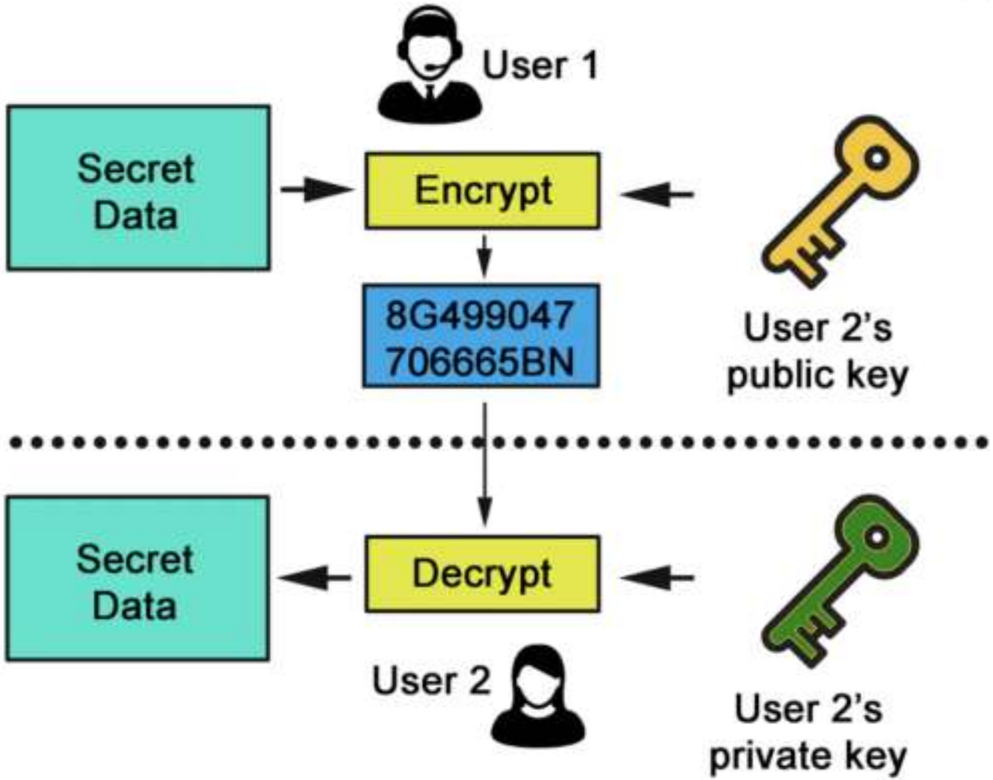
- Only one key is needed for each recipient

Public Key Distribution

- Only one key is needed for each recipient



n key pairs


User 1
Secret Data
Encrypt
8G499047 706665BN
User 2's public key
Secret Data
Decrypt
User 2
User 2's private key

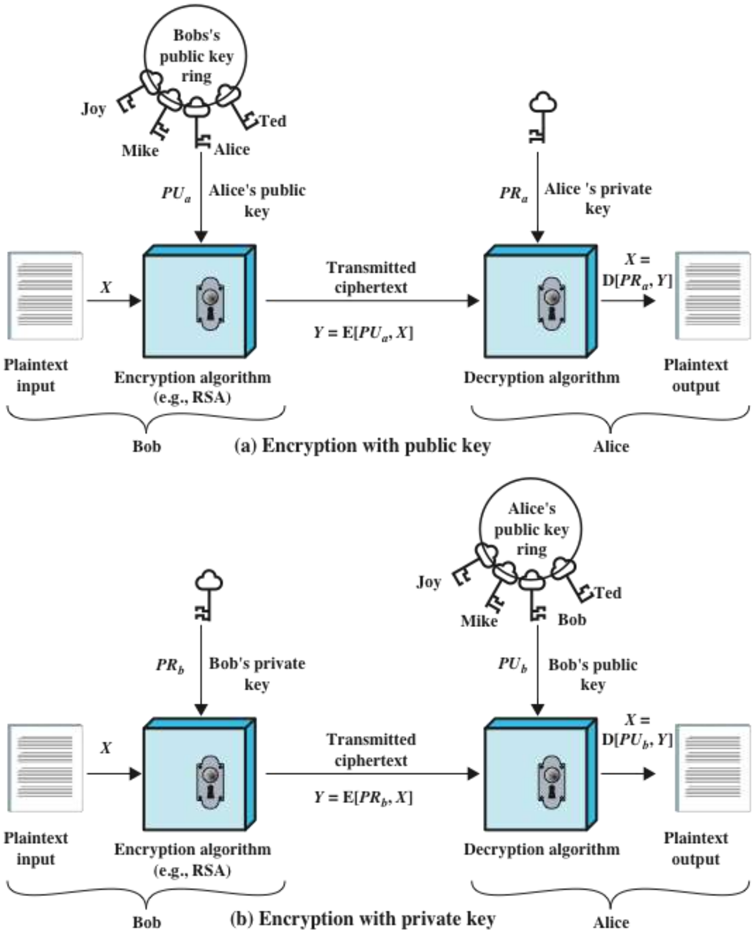
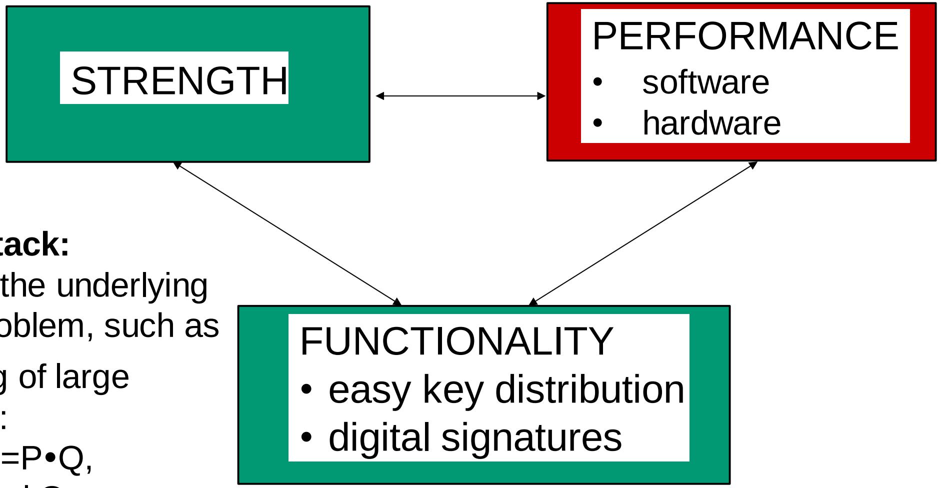


Figure 9.1 Public-Key Cryptography

Features of Public-Key Ciphers



Best attack:
Solving the underlying math problem, such as factoring of large integers:
Given N=P•Q,
find P and Q.

Primary Applications: Exchange of keys for secret-key ciphers
Digital signatures

Public Key conti..

- Examples:
  - Rivest Shamir Adleman (RSA)
    - Recommended key size: 1,024 to 4,096 bit typical
  - ElGamal encryption
- Computationally very expensive
  - Handling large message is ineffecient
  -

Message Authentication

- So far, we covered secrecy of the message and confidentiality.
  - message authentication is concerned with:
    - protecting the integrity of a
    - message validating identity of
    - originator
    - non-repudiation of origin (dispute resolution)
- Three alternative functions used
  - message encryption
  - message authentication code
  - (MAC) hash function

Message Authentication

- Message authentication is a mechanism or service used to verify the integrity of a message.
- Message authentication assures that data received are exactly as sent by (i.e., contain no modification, insertion, deletion, or replay) and
- that the purported identity of the sender is valid

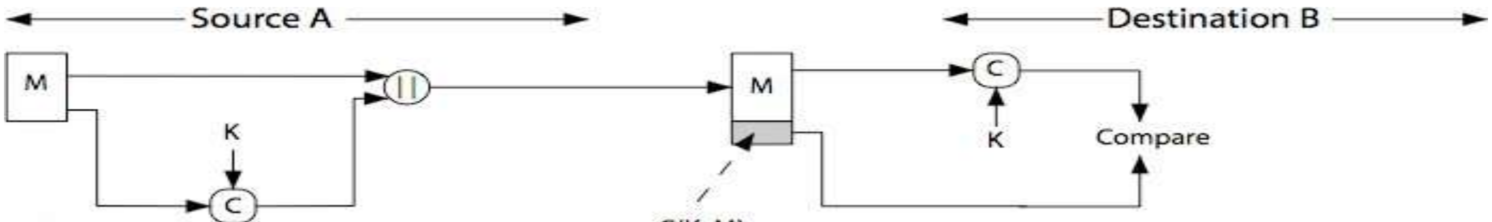
Authentication Functions

- Message encryption: The ciphertext of the entire message serves as its authenticator
- Message authentication code (MAC): A function of the ***message and a secret key that produces a fixed-length value*** that serves as the authenticator
- Hash function: A function that maps a ***message of any length into a fixed-length hash value***, which serves as the authenticator

Message Authentication Code (MAC)

- Allows for Alice and Bob to have data integrity, if they share a secret key.
- Generated by an algorithm that creates a small fixed-sized block depending on both message M and some secret key K s.t. MAC = C(K,M), where
  - M = input message
  - C = MAC function
  - K = shared secret key
  - MAC = message authentication code
- Appended to message as a **signature**
- Receiver performs same computation on message and checks it matches the MAC
- Provides assurance that message is unaltered and comes from sender

MAC conti…

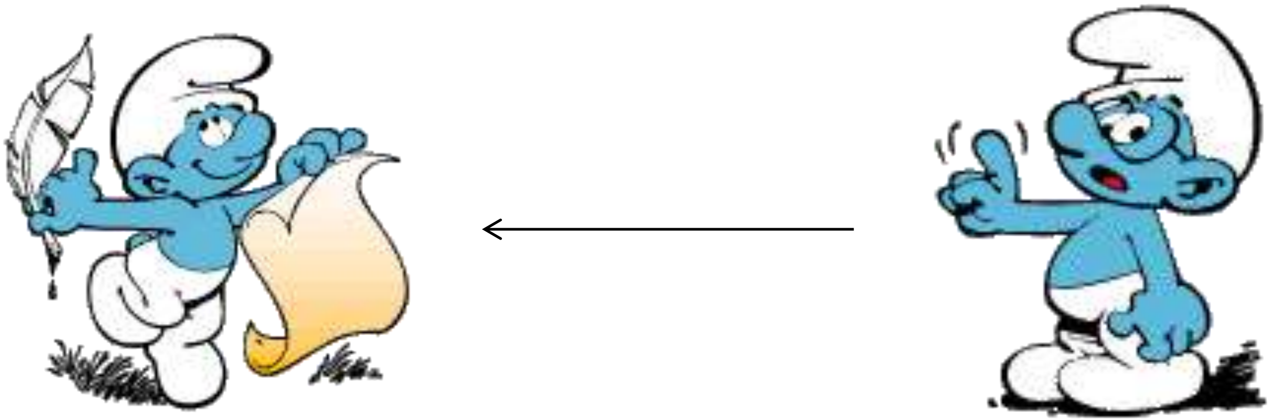


(a) Message authentication

Digital Signatures

- Public-key encryption provides a method for doing digital signatures
- To sign a message, M, Alice just encrypts it with her private key, SA, creating $C = E_{SA}(M)$.
- Anyone can decrypt this message using Alice's public key, as $M' = D_{PA}(C)$, and compare that to the message M.

Digital Signature Problem



Both corresponding sides have the same information and are able to generate a signature

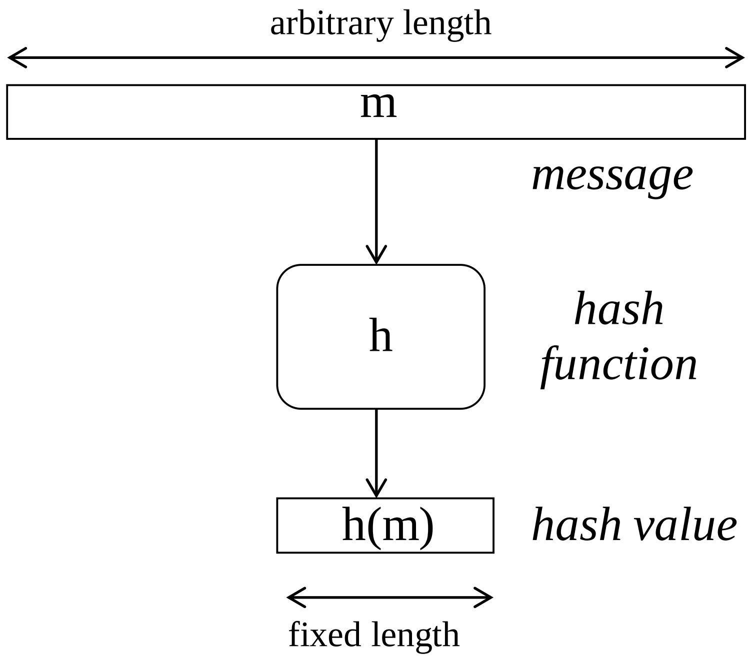
There is a possibility of the

- **receiver falsifying the message**
- **sender denying that he/she sent the message**

Cryptographic Hash Functions

- A checksum on a message, M, that is:
- **One-way**: it should be easy to compute Y=H(M), but hard to find M given only Y
- **Collision-resistant:** it should be hard to find two messages, M and N, such that H(M)=H(N).
- **Examples:** SHA-1, SHA-256.

Hash function



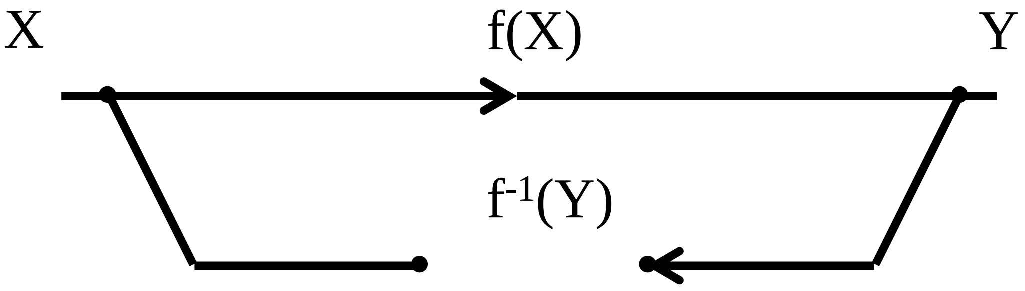
Hash functions

Security requirements

It is computationally infeasible

Property	**Given**	**To Find**
One-way	$\boldsymbol{h(m)}$	$\boldsymbol{m}$
Weak collision resistant	$\boldsymbol{m}$ and $\boldsymbol{h(m)}$	$\boldsymbol{m' \neq m}$, such that $\boldsymbol{h(m') = h(m)}$
Strong collison resistant		$\boldsymbol{m' \neq m}$, such that $\boldsymbol{h(m') = h(m)}$

One-way function



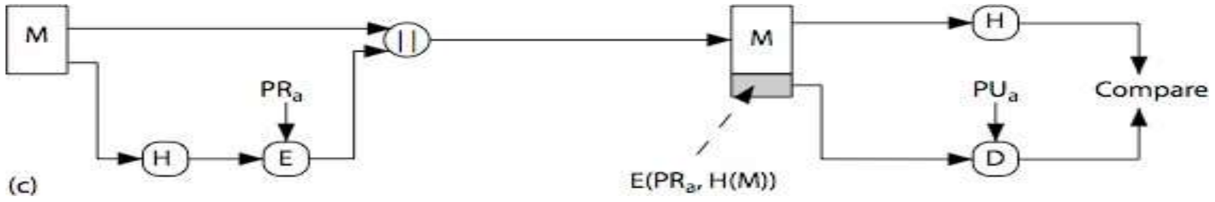
EXAMPLE:

$$f\colon Y = f(X) = A^X \bmod P$$

where P and A are constants, P is a large prime,
A is an integer smaller than P

Number of bits of P	**Average number of multiplications necessary to compute**	
	f	**f^{-1}**
1000	1500	10^{30}

Application of Hash



Public Distribution of Secret Keys

- Public-key algorithms are slow
- *So we usually want to use symmetric key encryption to protect message contents*
- Hence need to share secret (session) key
- There are alternatives for negotiating a suitable session

Diffie-Hellman Key Exchange

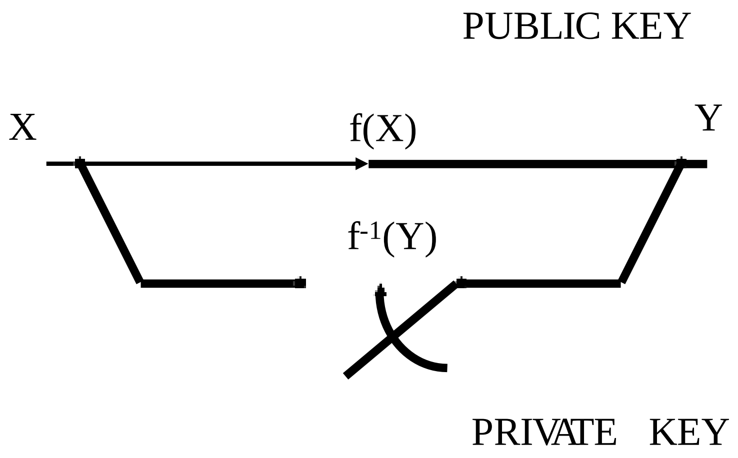
- First public-key type scheme proposed by Diffie & Hellman in 1976 along with the exposition of public key concepts[1]
- Practical method for public exchange of a secret
- key

Used in a number of real-world commercial products/protocols

1. Now know that Williamson (UK CESG) secretly proposed the concept in 1970

Trap-door one-way function

Whitfield Diffie and Martin Hellman
"*New directions in cryptography,*" 1976



Diffie-Hellman Key Exchange

- a public-key distribution scheme
  - cannot be used to exchange an arbitrary message
  - rather it can establish a common key
  - known only to the two participants
- value of key depends on the participants (and their private and public key information)
- security relies on the difficulty of computing discrete logarithms (similar to factoring) – hard

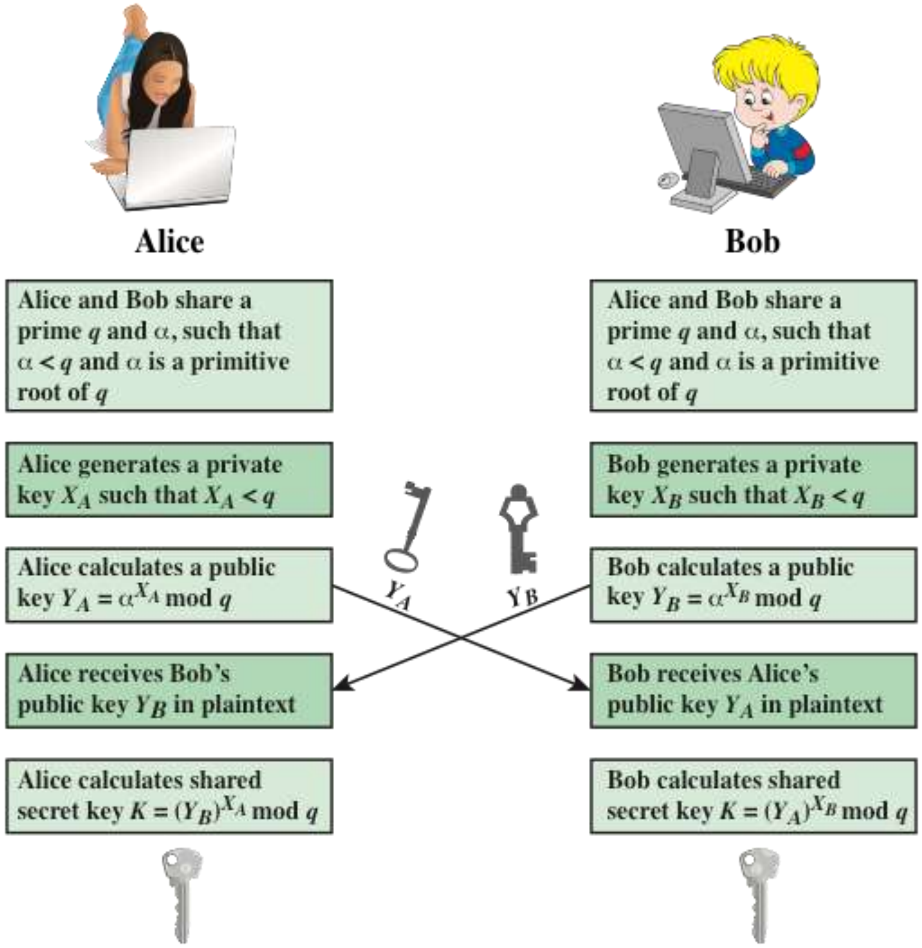


Figure 10.1 Diffie-Hellman Key Exchange

Cryptography and Network Security, Seventh Edition by William Stallings