Cryptography and Network Security (CS435/890BN)

Part One

(Introduction)

Background

- Information Security requirements have changed in recent years
- Traditionally provided by physical and administrative mechanisms
- Computer use requires automated tools to protect files and other stored information
- Use of networks and communications links requires measures to protect data during transmission

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

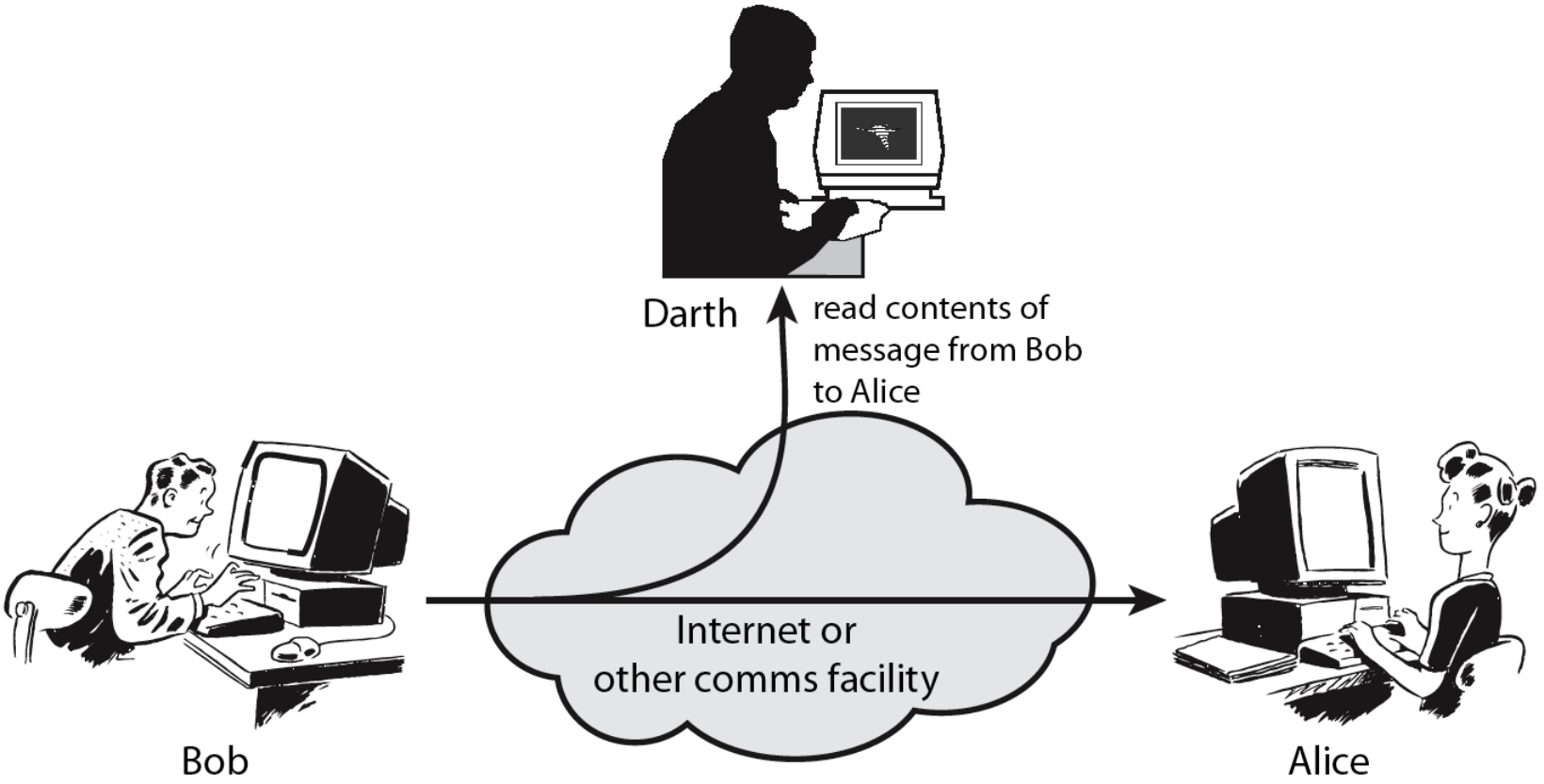
Aspects of Security

- Consider 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**

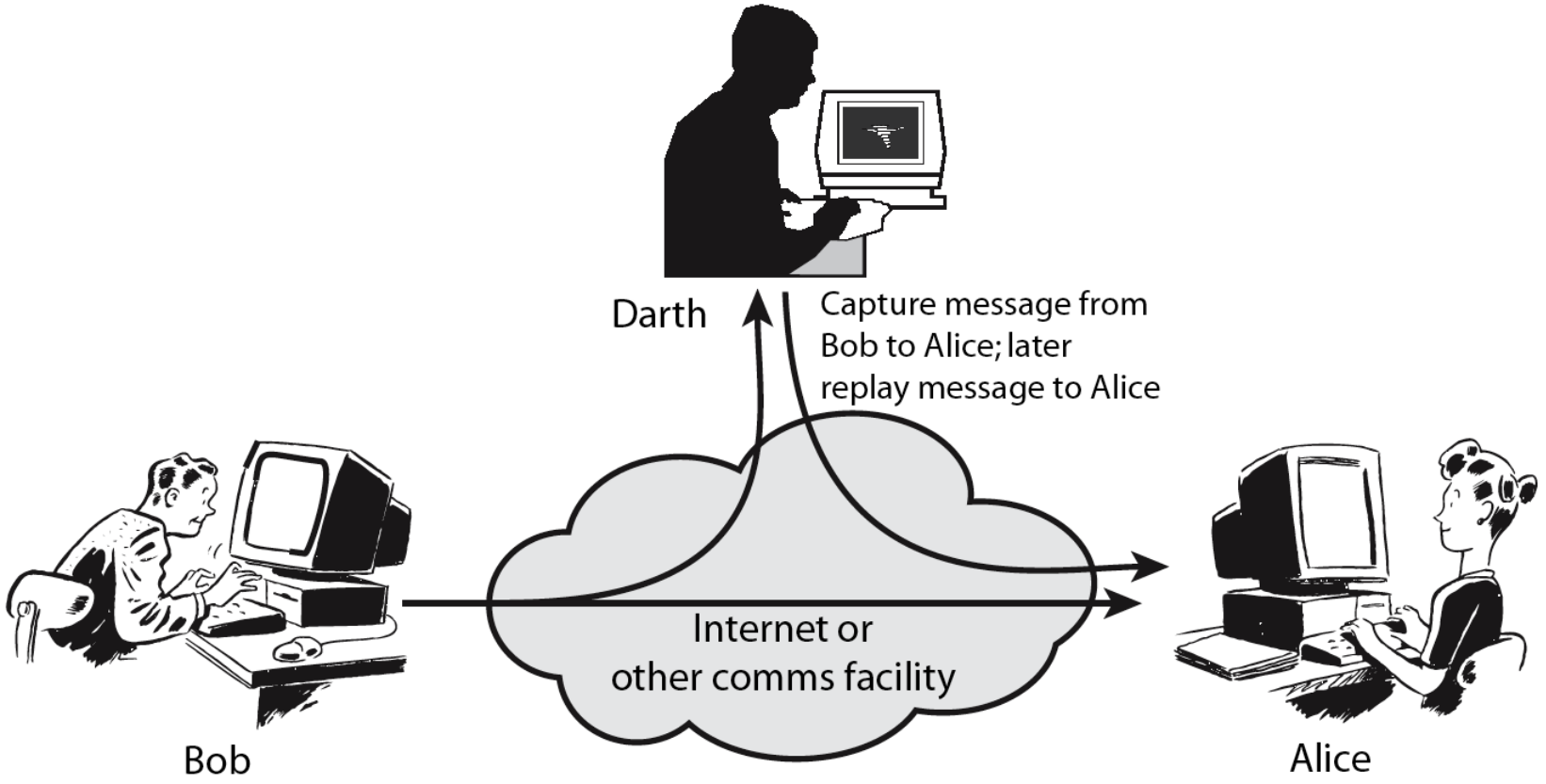
Security Attack

- Any action that compromises the security of information owned by an organization
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- Often *threat* & *attack* used to mean same thing
- Have a wide range of attacks
- Can focus of generic types of attacks
  - passive
  - active

Passive Attacks



Active Attacks



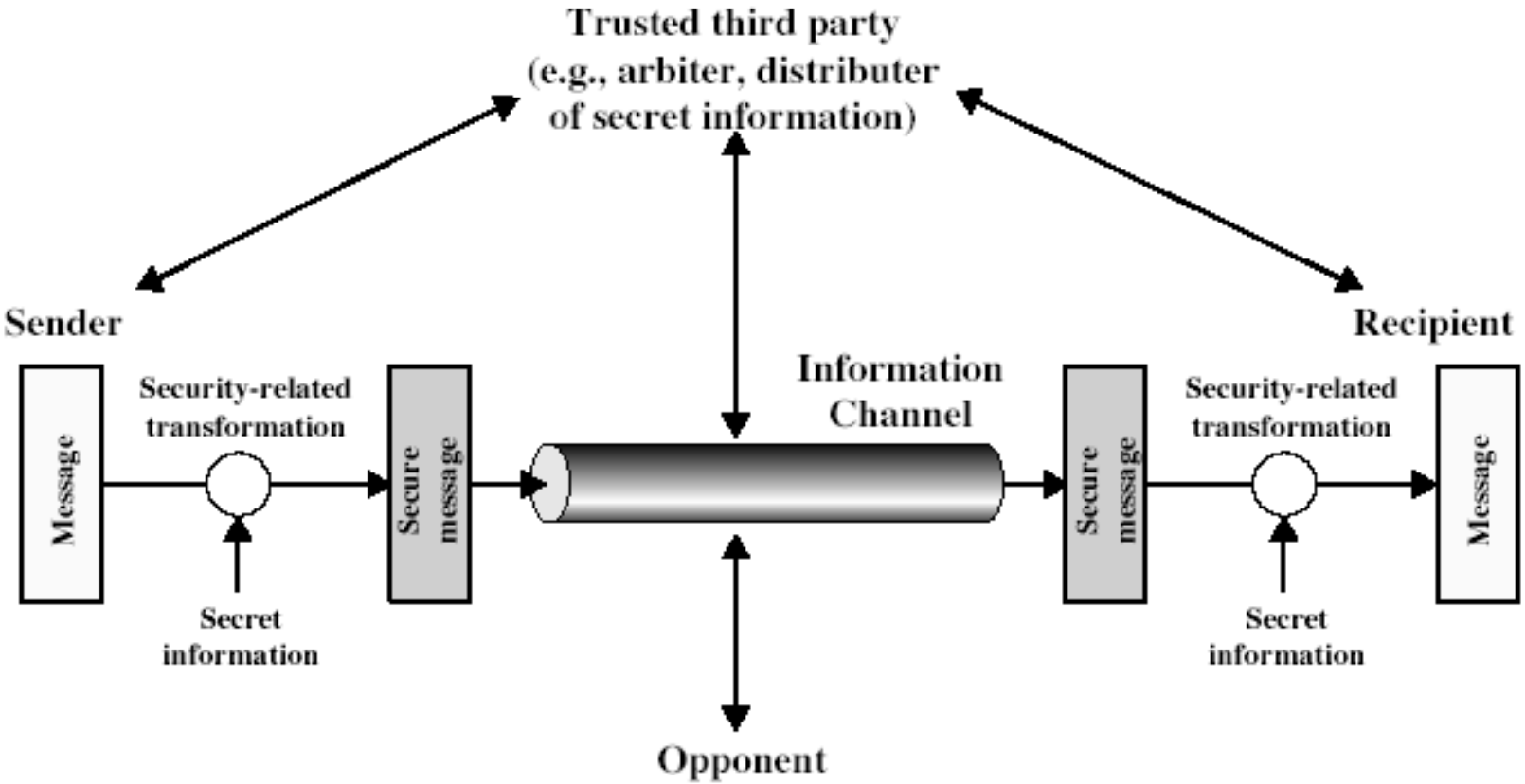
Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic

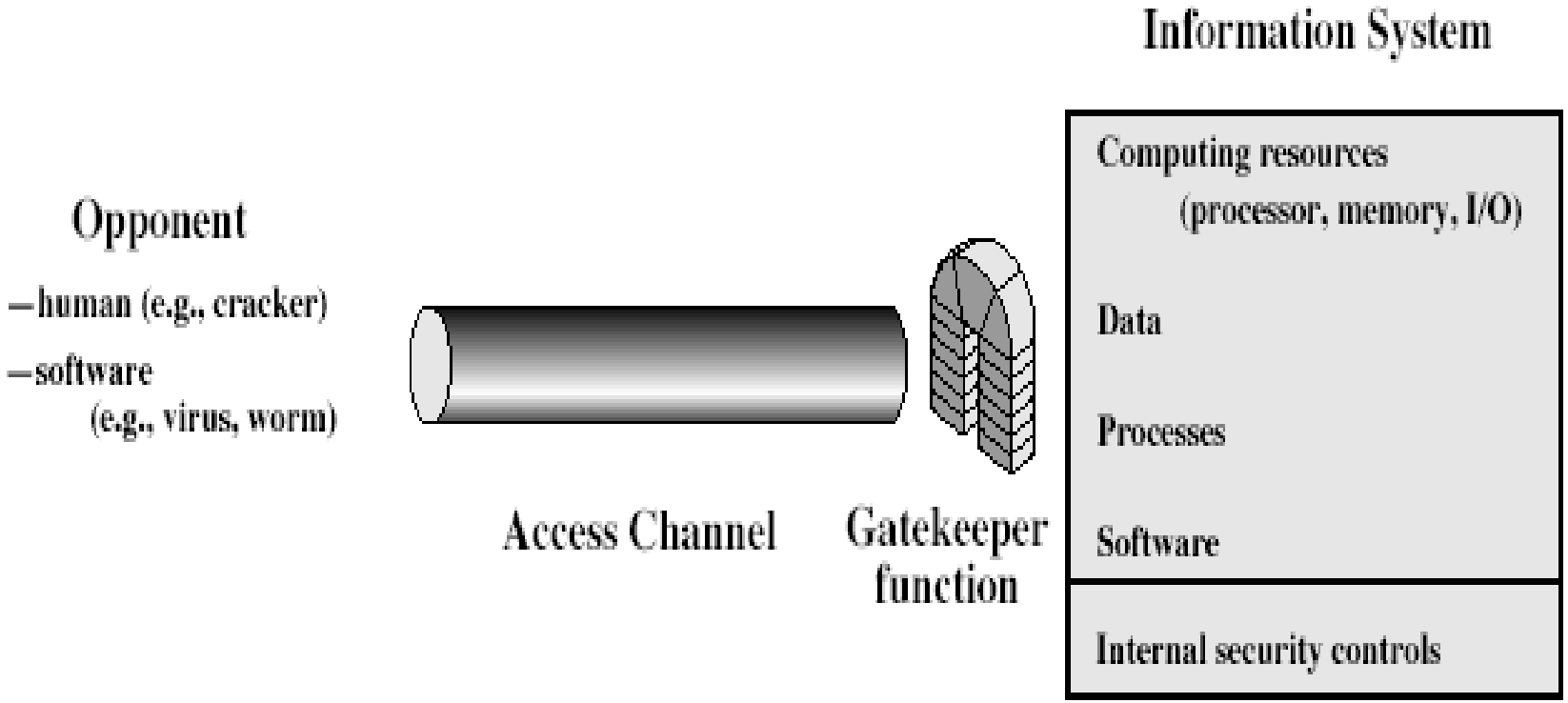
Model for Network Security



Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems may be useful to help implement this model

Quick Overview

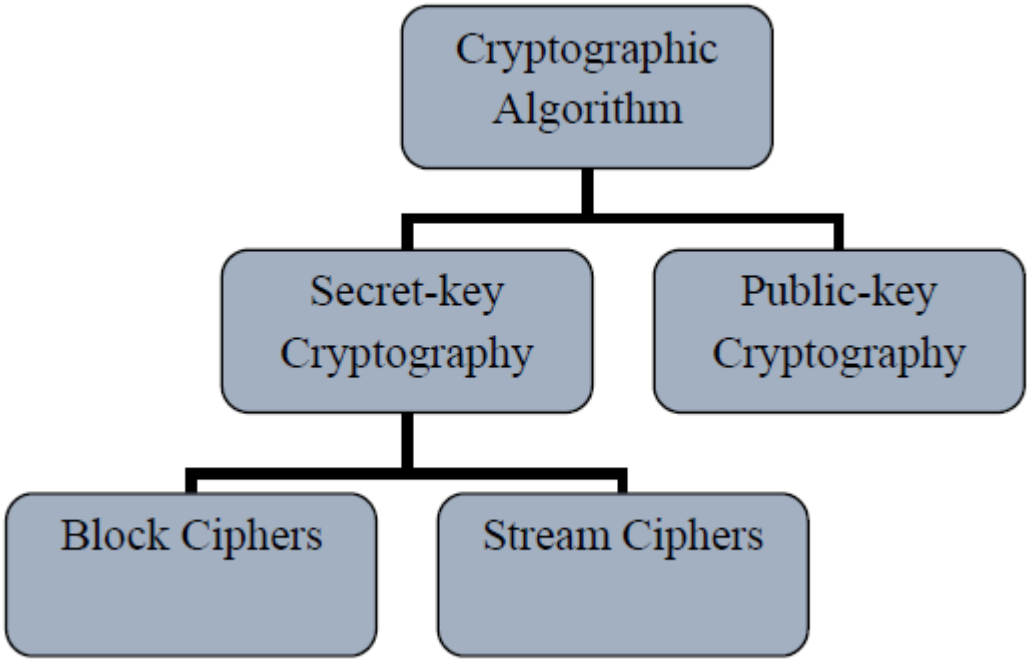
Key Concepts

- Data confidentiality: keeps the contents of information hidden from all but authorized ones. It is also called privacy or secrecy.
  - Method: Encryption / decryption

Key Concepts cont.

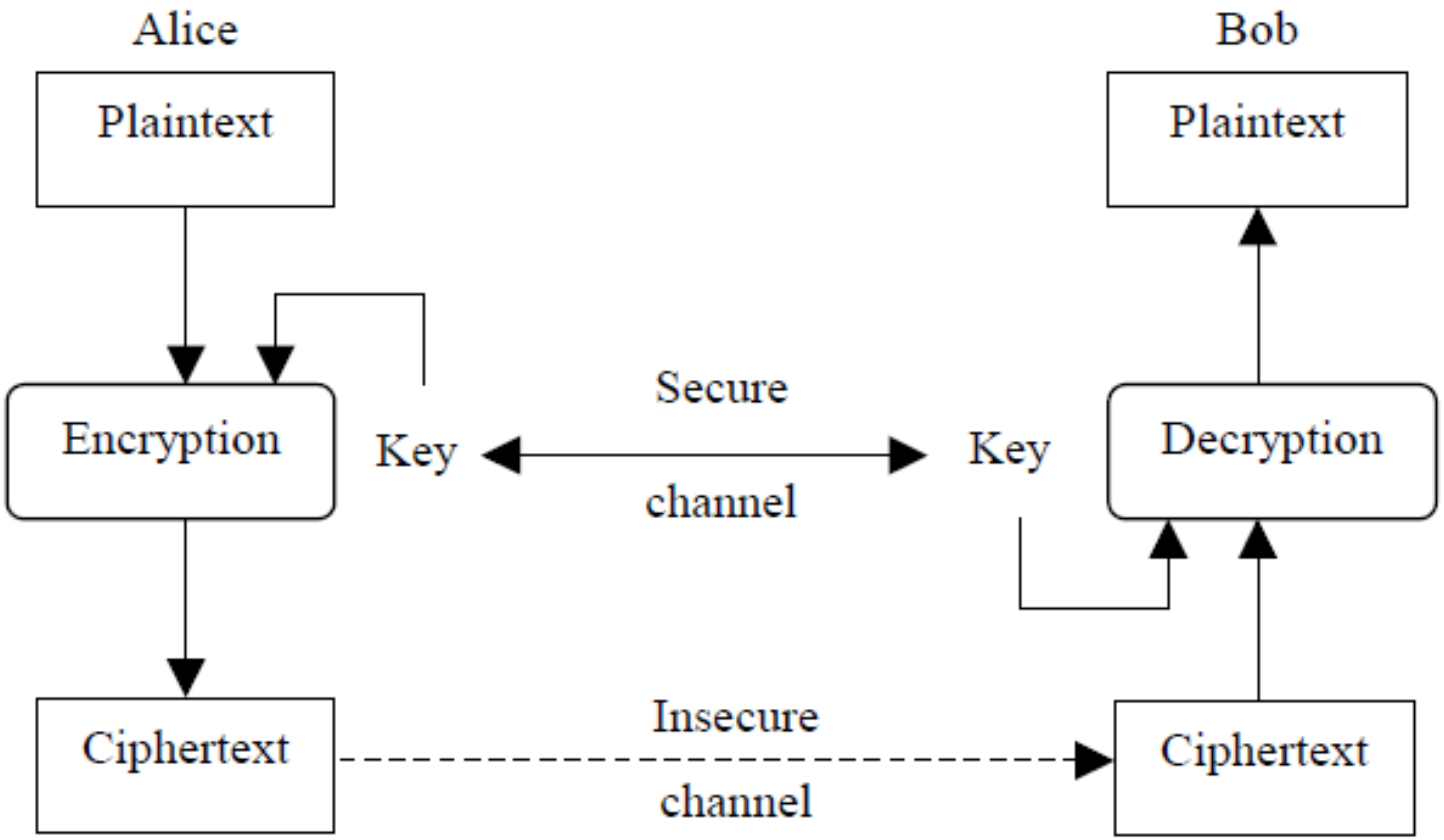
- Authentication: assure the receiver receives the message come from the source where it claims to be from
- Access Control: limit and control the access to host systems and applications via communications links
- Data Integrity: assure the message has not been modified in the transmission
- Data freshness: assure the message is fresh.

General Structure of the Cryptographic Algorithm

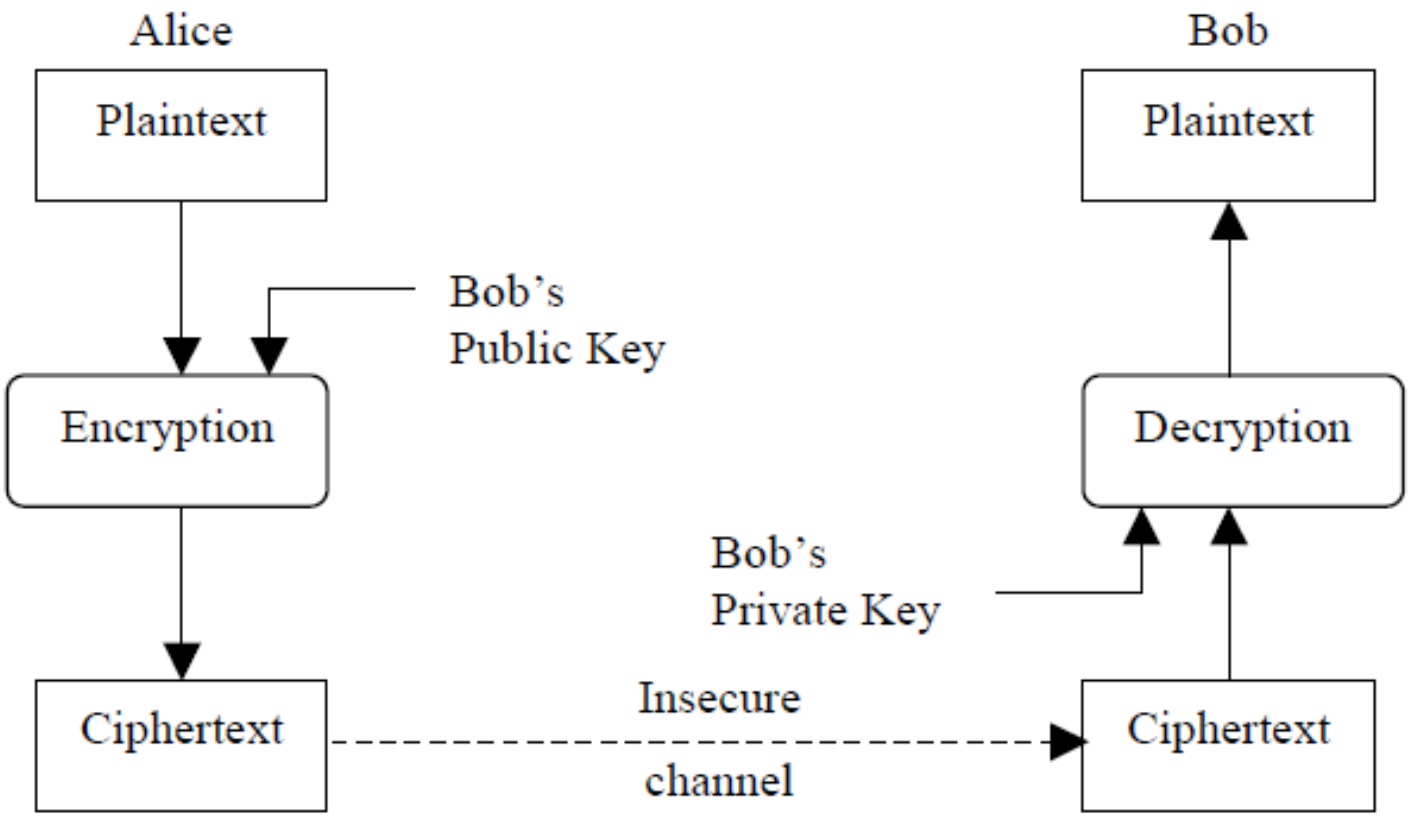


Note: While most stream ciphers are in Secret-key Cryptography, some do not.

Secret-key cryptography



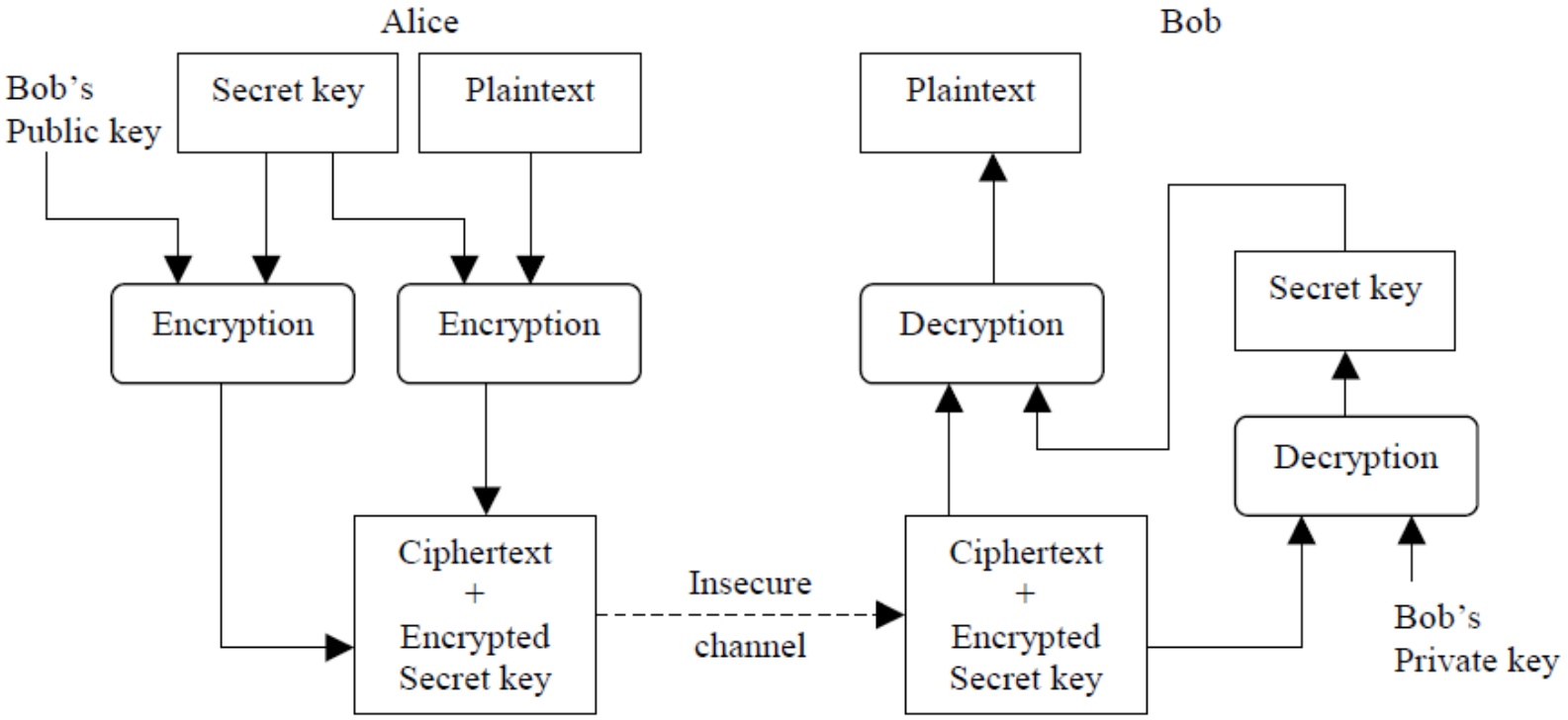
Public-key cryptography



Hybrid cryptosystem

- The combination of public-key and secret-key cryptosystems in order to obtain both the security advantages of public-key cryptosystems and the speed advantages of secret-key cryptosystems.
- The plaintext is encrypted with a secret key cipher and the secret key is protected by a public-key cipher.

Hybrid cryptosystem cont.



Block cipher & Stream cipher

- In the block cipher, the plaintext is divided into blocks of fixed length which then are encrypted into blocks of ciphertext of the same length. Decryption is performed by applying the reverse transformation to the ciphertext block using the same secret key. For example, DES (data encryption standard), and AES (advanced encryption standard)

Block cipher & Stream cipher cont.

- Stream ciphers encrypt each digit of plaintext one at a time, using a simple time-dependent encryption transformation. In practice, the digit is typically single bit or byte.

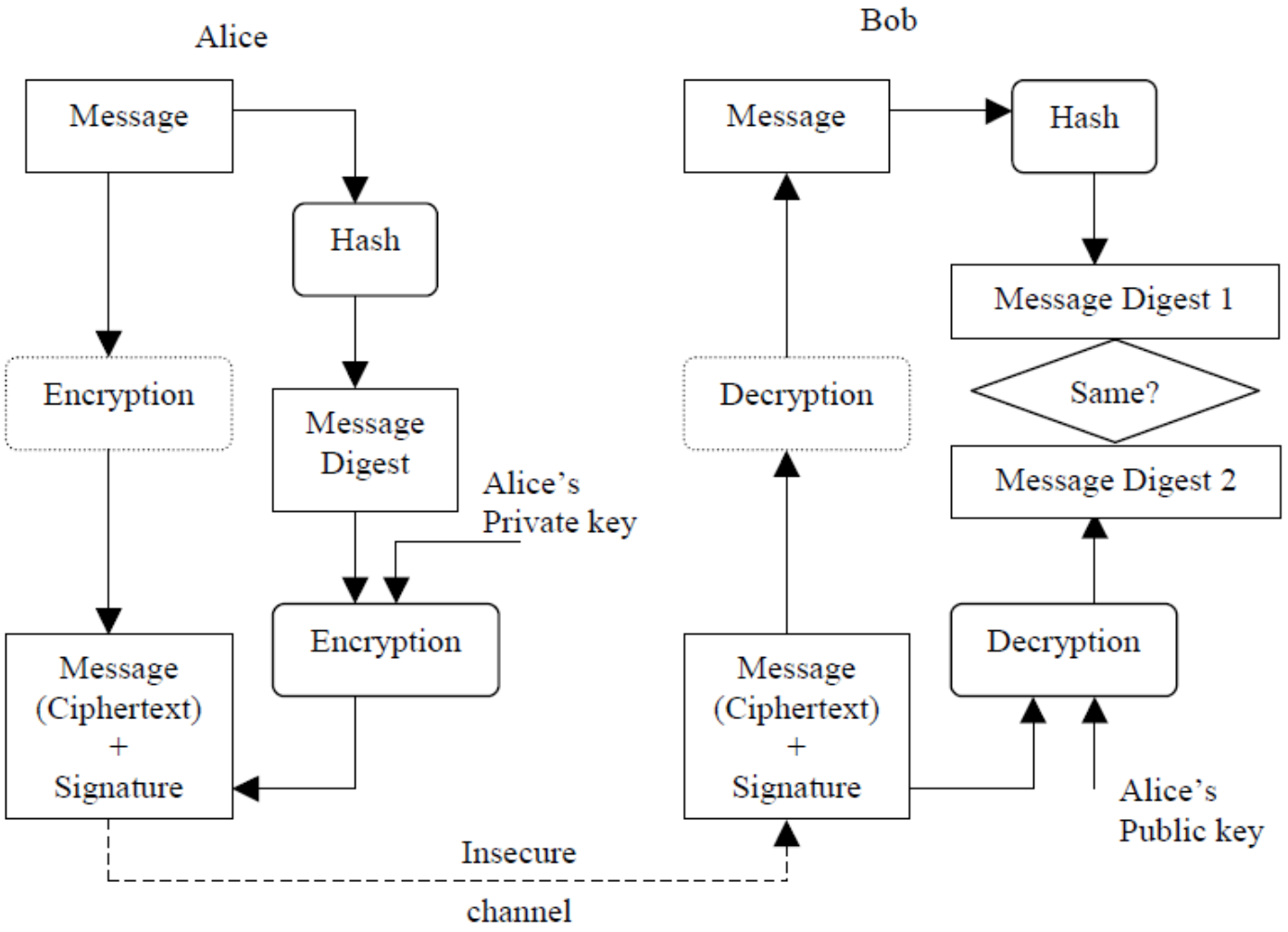
One-way hash function

- A hash function H is a transformation that takes an input m and returns a fixed-size string, which is called the hash value h (that is, h=H(m)).
- Hash functions with just this property have a variety of general computational uses, but when employed in cryptography, the hash functions are usually designed to have some additional properties.

Digital signatures

- The digital signature of a document is a piece of information based on both the document and the signer's private key for the purpose of authentication, which is typically created through the use of a hash function and a private signing function (encrypting the hash value with the signer's private key).

Digital signatures cont.

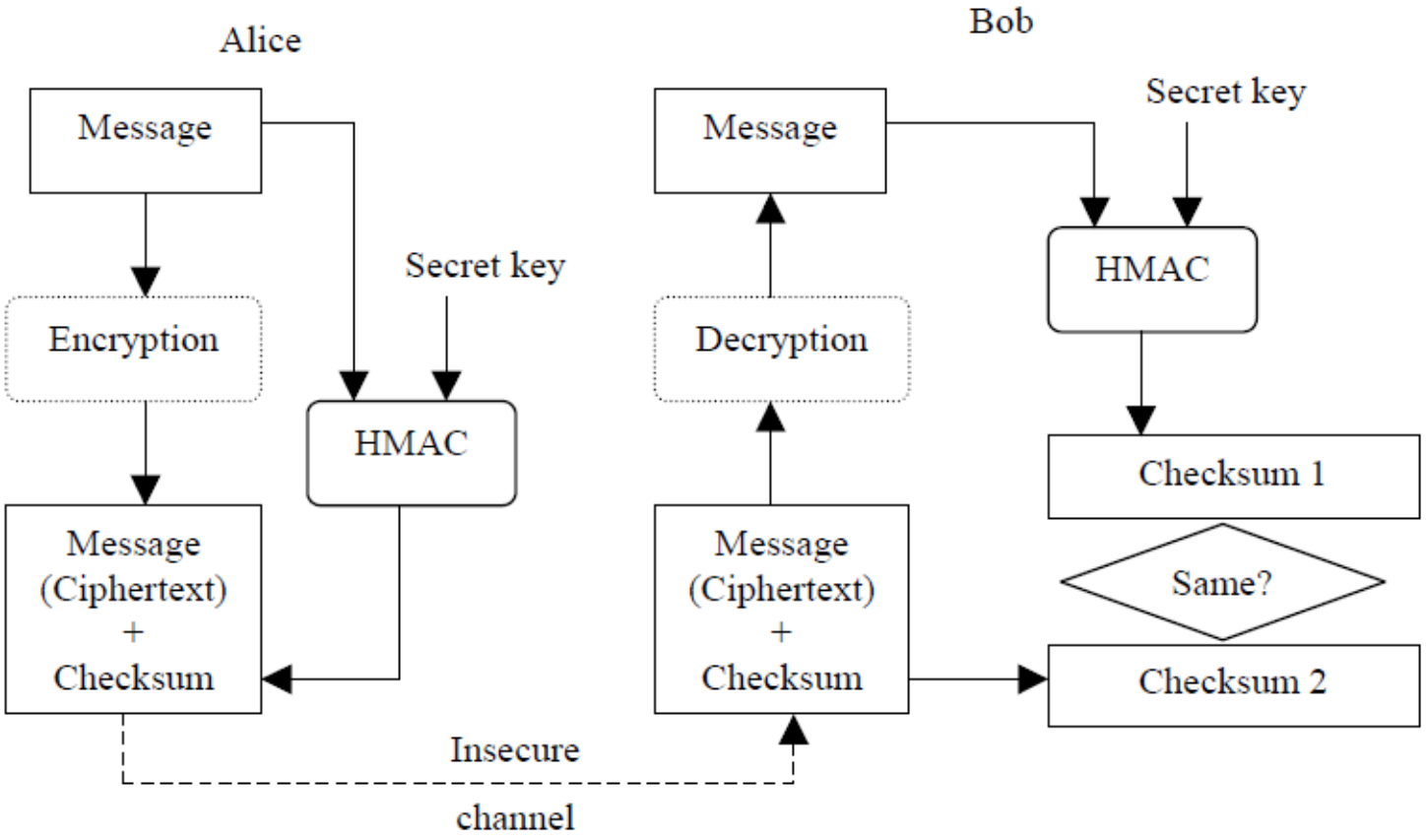


Message Authentication Codes

- Message Authentication Code is another mechanism to achieve authentication.
- A message authentication code is a checksum derived by applying an authentication scheme, together with a secret key, to a message.
- MACs are computed and verified with the same key.

Message Authentication Codes

cont.



Secure Unicast