Introduction to Information Technology

CSC109

2020

By: Rajiv Raman Parajuli

CRYPTOGRAPHY

- Cryptography derived its name from a Greek word called "krypto's" which means "Hidden Secrets".
- Cryptography is the practice and study of hiding information. It is the Art or Science of converting a plain intelligible data into an unintelligible data and again retransforming that message into its original form.
- It uses the mathematics to encrypt and decrypt the information.
- It provides Confidentiality, Integrity, and Accuracy.
- cryptography provides security and makes only the aimed recipient to read the data.
- cryptology includes both the cryptography and cryptanalyst; cryptanalyst is called as attackers

Some terms commonly used in cryptography:

1. **Plaintext:** i.e. unencrypted data.
2. **Cipher and Code:** Cipher is a bit-by-bit or character-by-character transformation without regard to the meaning of the message. Code replaces one word with another word or symbol. Codes are not used any more.
3. **Cipher text:**
4. **Encryption:**
5. **Decryption:**

Purpose Of Cryptography

- **Authentication:** The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- **Privacy/confidentiality:** Ensuring that no one can read the message except the intended receiver.
- **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation:** A mechanism to prove that the sender really sent this message.

Key

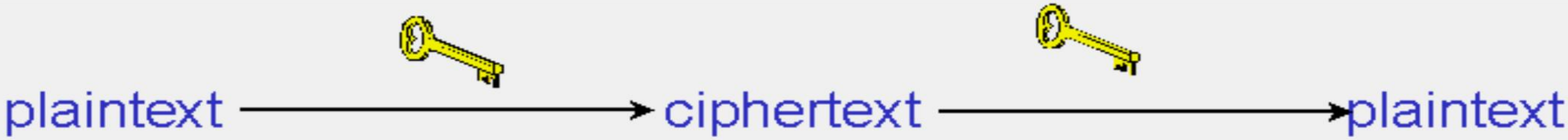
Key is a secret parameter (string of bits) for a specific message exchange context.

Keys are important, as algorithms without keys are not useful. The encrypted data cannot be accessed without the appropriate key.

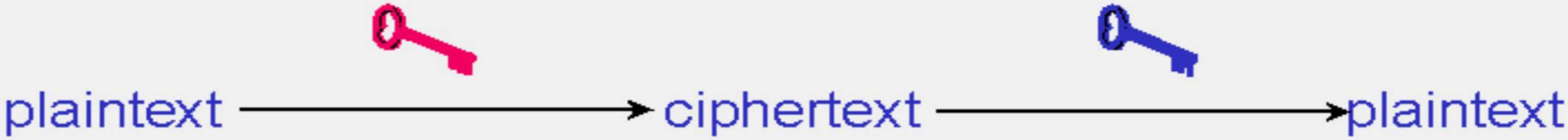
The size of key is also important. The larger the key, the harder it is to crack a block of encrypted data.

The algorithms differ based on the number of keys that are used for encryption and decryption.

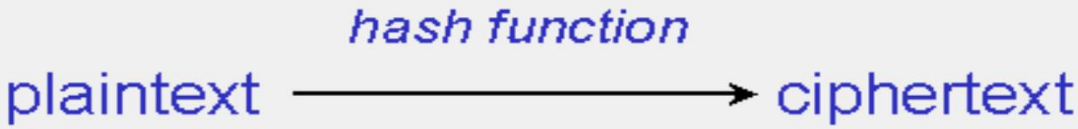
1. Secret Key Cryptography (SKC)
2. Public Key Cryptography (PKC)
3. Hash Functions



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

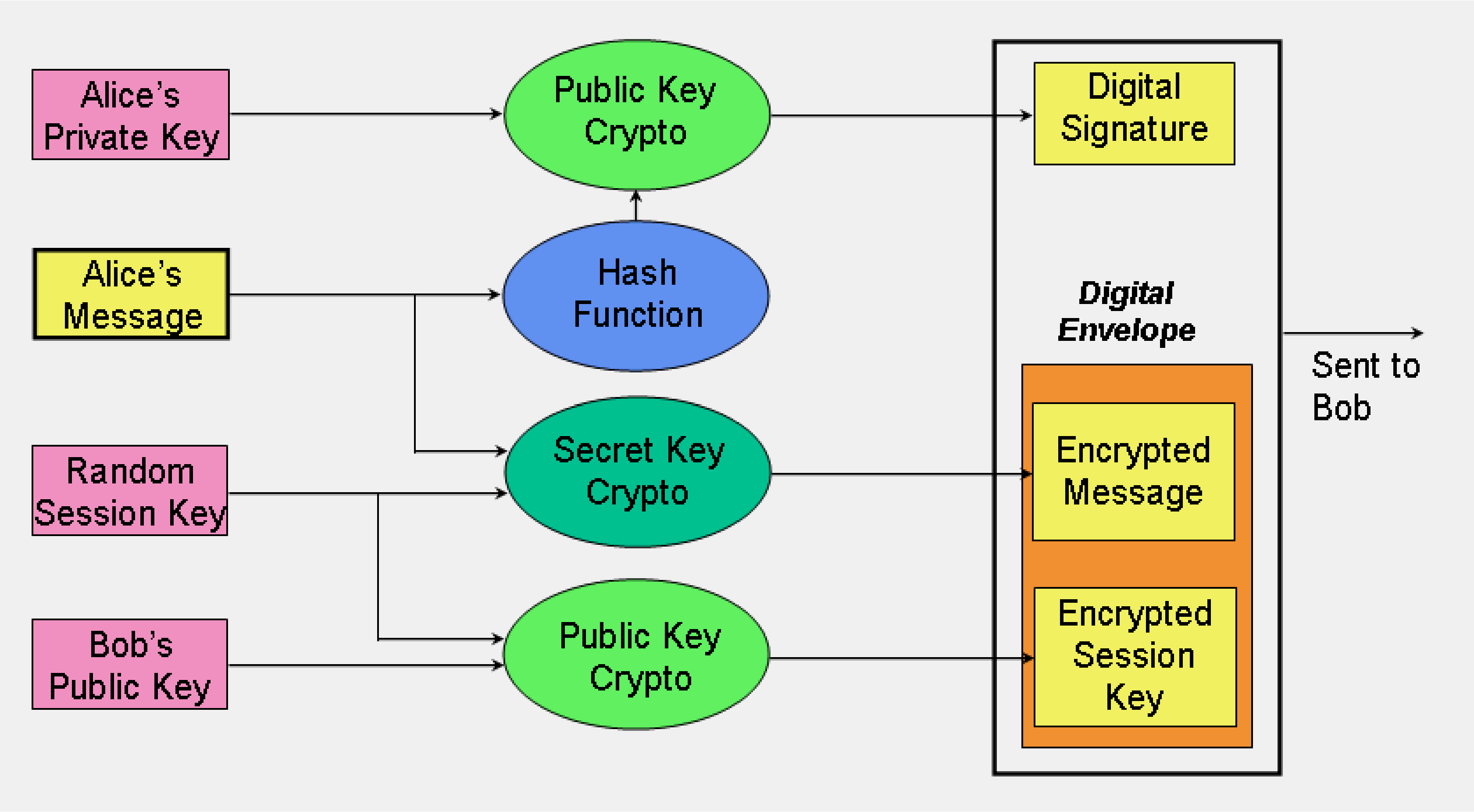


B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.



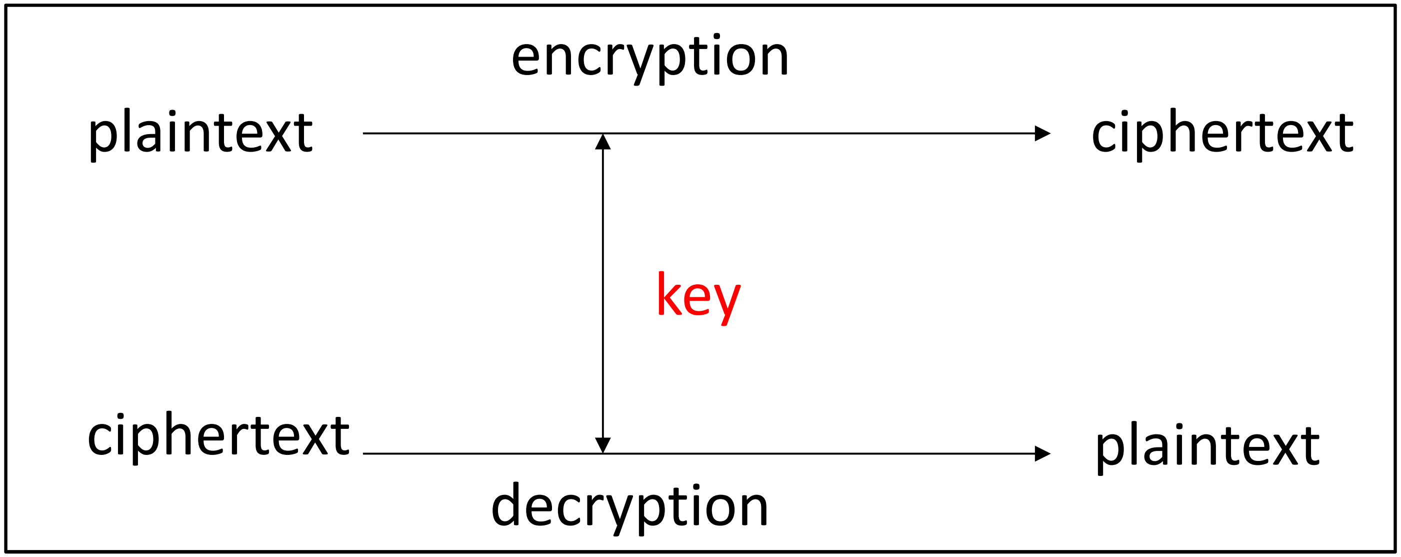
C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Architecture of cryptography



Secret Key Cryptography/ symmetric encryption.

- Single key used to encrypt and decrypt.
- Key must be known by both parties.
- Assuming we live in a hostile environment (otherwise - why the need for cryptography?), it may be hard to share a secret key.
- Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are some of the secret key cryptography algorithms that are in use nowadays.



encryption

plaintext

ciphertext

key

ciphertext

plaintext

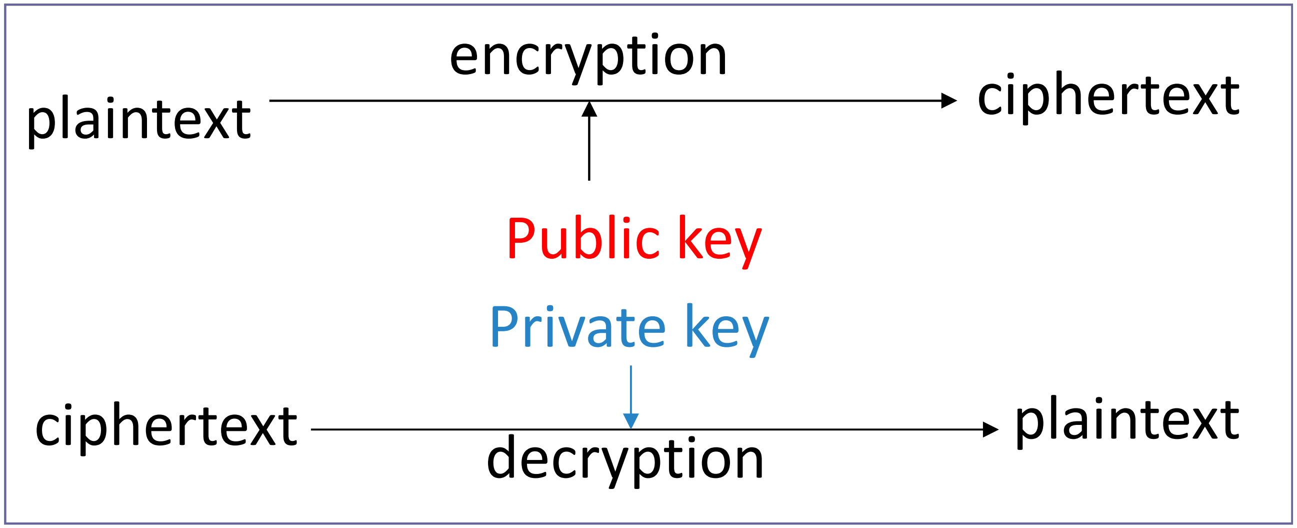
decryption

Public-Key Cryptography asymmetric encryption

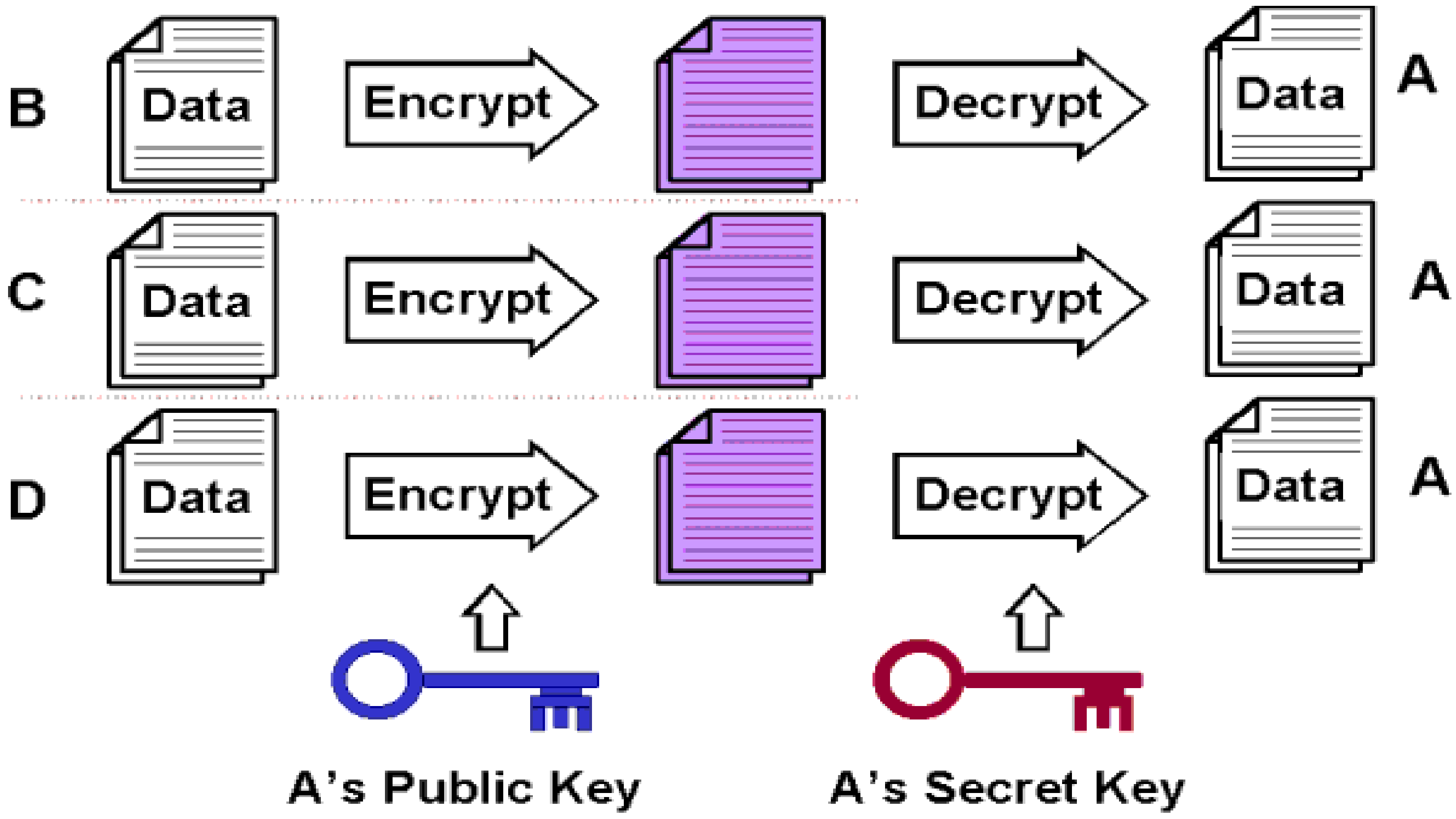
One of the keys allocated to each person is called the "public key", and is published in an open directory somewhere where anyone can easily look it up, for example by email address.

Each entity has 2 keys: Private Key (a secret) Public key (well known).

Private keys are used for decrypting. Public keys are used for encrypting



- Asymmetric key cryptography overcomes the key management problem by using different encryption and decryption key pairs. Having knowledge of one key, say the encryption key, is not sufficient enough to determine the other key - the decryption key.
- The mathematical relationship between the public/private key pair permits a general rule: any message encrypted with one key of the pair can be successfully decrypted only with that key's counterpart.


B
Data
Encrypt
Decrypt
Data
A
C
Data
Encrypt
Decrypt
Data
A
D
Data
Encrypt
Decrypt
Data
A
A's Public Key
A's Secret Key

Hash Functions

- Hash function (have no key since plain text is not recoverable from cipher text)
- Hash functions are one-way encryption algorithms
- A mathematical transformation that takes a message of arbitrary length and computes it a fixed-length (short) number.
- Hash functions are generally used to ensure that the file has not been altered by an intruder or virus.
- Hash functions are commonly employed by many operating systems to encrypt passwords. Message Digest (MD) algorithm and Secure Hash Algorithm (SHA) are some of the common used hash algorithms.

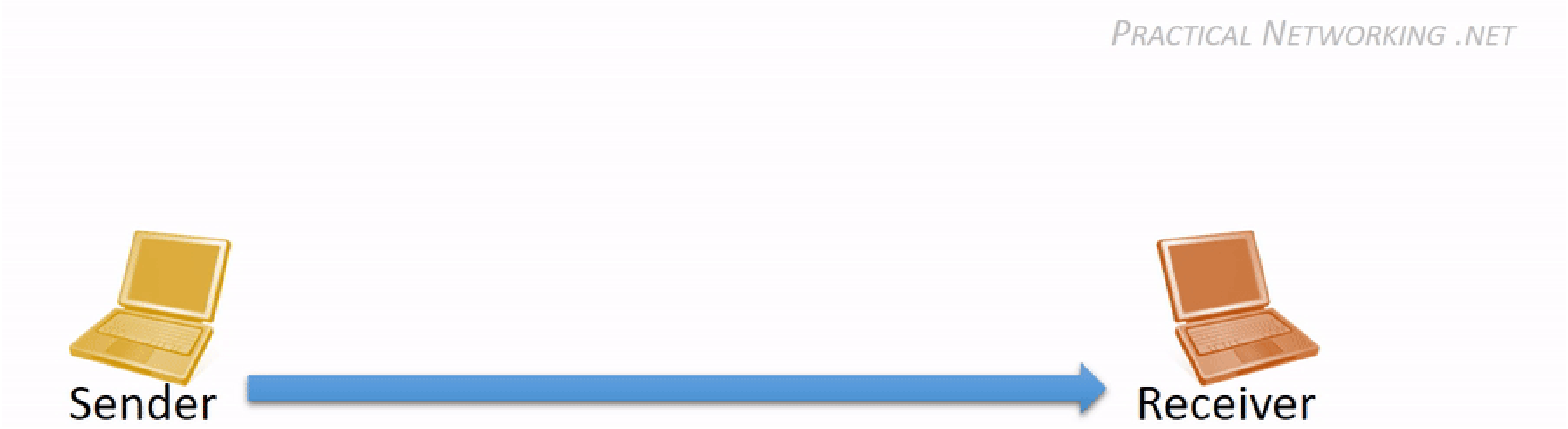
Password hashing

- The system store a hash of the password (not the password itself)
- When a password is supplied, it computes the password’s hash and compares it with the stored value.

Message integrity

- Using cryptographic hash functions to generate a MAC

PRACTICAL NETWORKING .NET
Sender
Receiver


PRACTICAL NETWORKING .NET
Sender
Receiver

DIGITAL SIGNATURE

FIREWALL

Types of Firewall

Packet Filter Firewall

Circuit Filter Firewall

Application-Level Gateway

USERS IDENTIFICATION & AUTHENTICATION

User Name and Password

Smart Card

Biometric Techniques

OTHER SECURITY MEASURES

SECURITY AWARENESS

SECURITY POLICY

Formulating a Security Policy