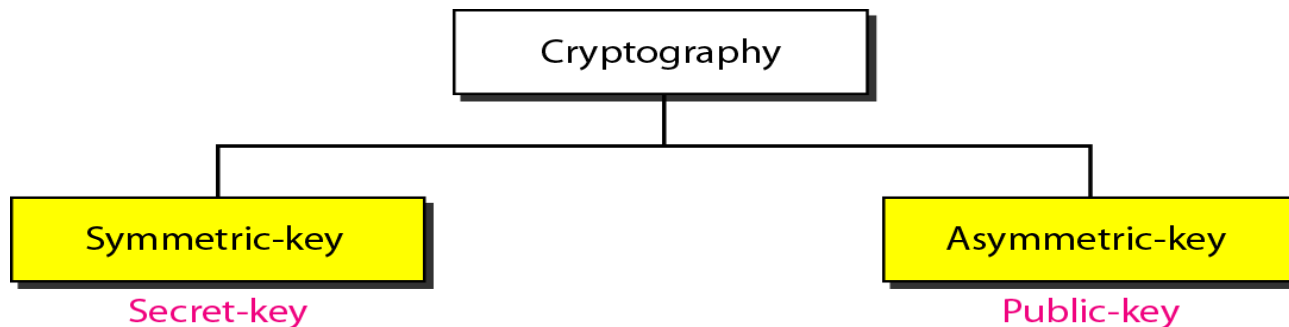


Chapter two part 2

Categories of cryptography

We can divide all the cryptography algorithms (ciphers) into two groups:

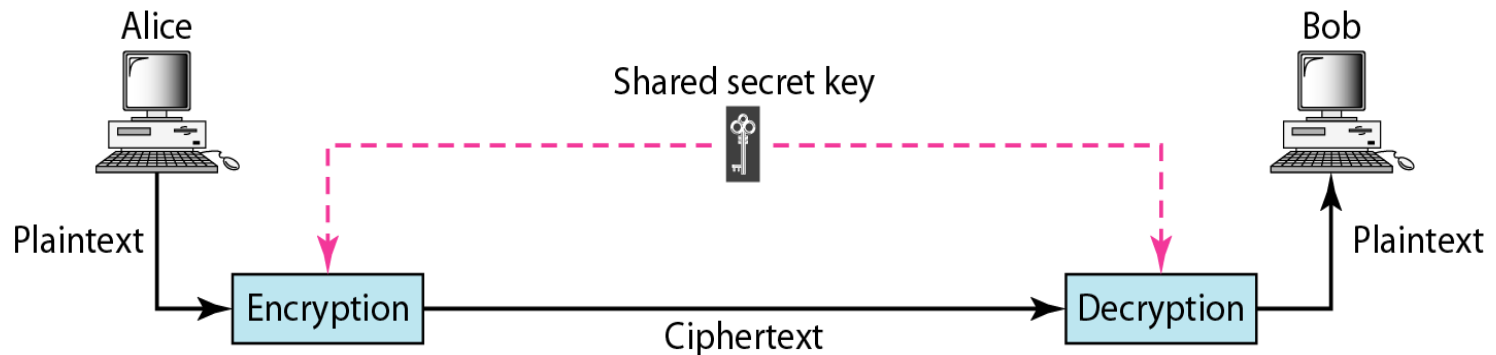
- **symmetric** key(also called secret-key) cryptography algorithms. E.g. Caesar Cipher
- **asymmetric** (also called public-key) cryptography algorithms.



Symmetric-key cryptography

- In symmetric-key cryptography, the same key is used by both parties.
- The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

The key is shared



Types of Symmetric Encryption

- Algorithms in which the key for encryption and decryption are the same in Symmetric
Example: Caesar Cipher

Types:

1. Block Ciphers

- Encrypt data one block at a time
(typically 64 bits, or 128 bits)
- Used for a single message

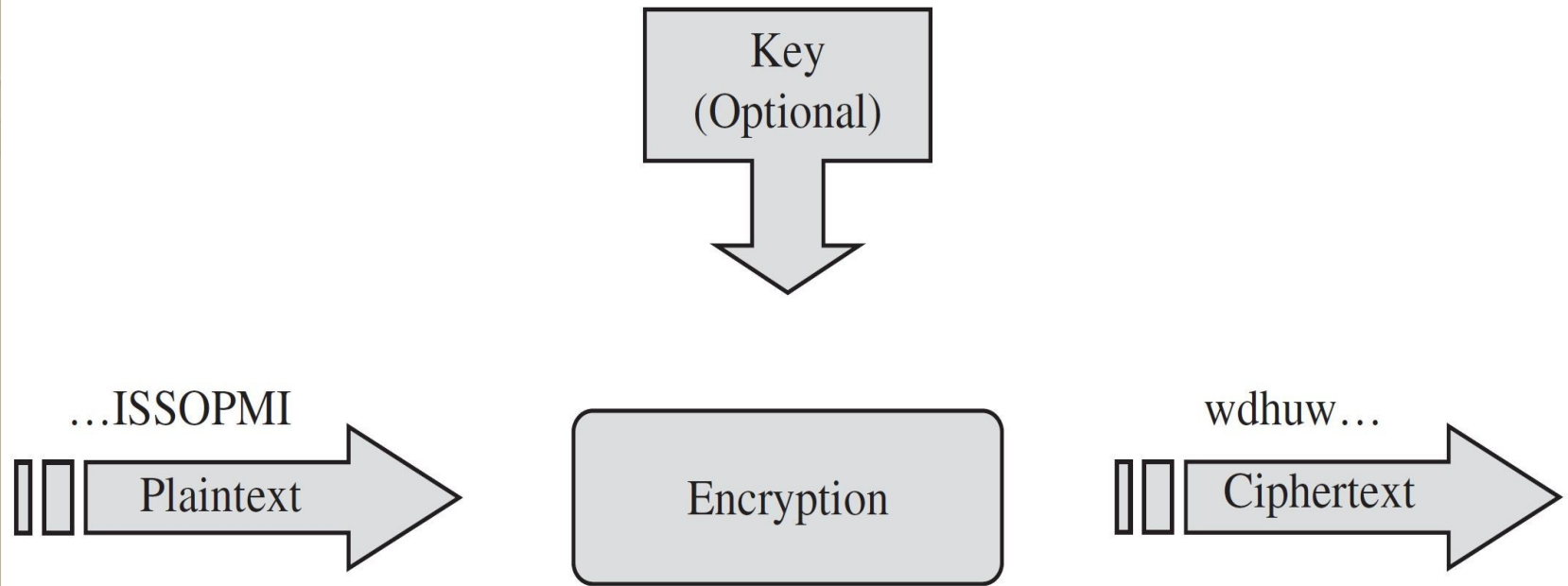
2. Stream Ciphers

- Encrypt data one bit or one byte at a time
- Used if data is a constant stream of information

STREAM CIPHER

- Stream cipher is a symmetric key cipher where plaintext digits are combined with a **pseudo-random cipher digit stream (keystream)**.
- In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream.
- An alternative name is a **state cipher**, as the encryption of each digit is dependent on the current state.
- In practice, a digit is typically a bit and the combining operation an exclusive-or (xor).
- Good for real-time services.

STREAM ENCRYPTION

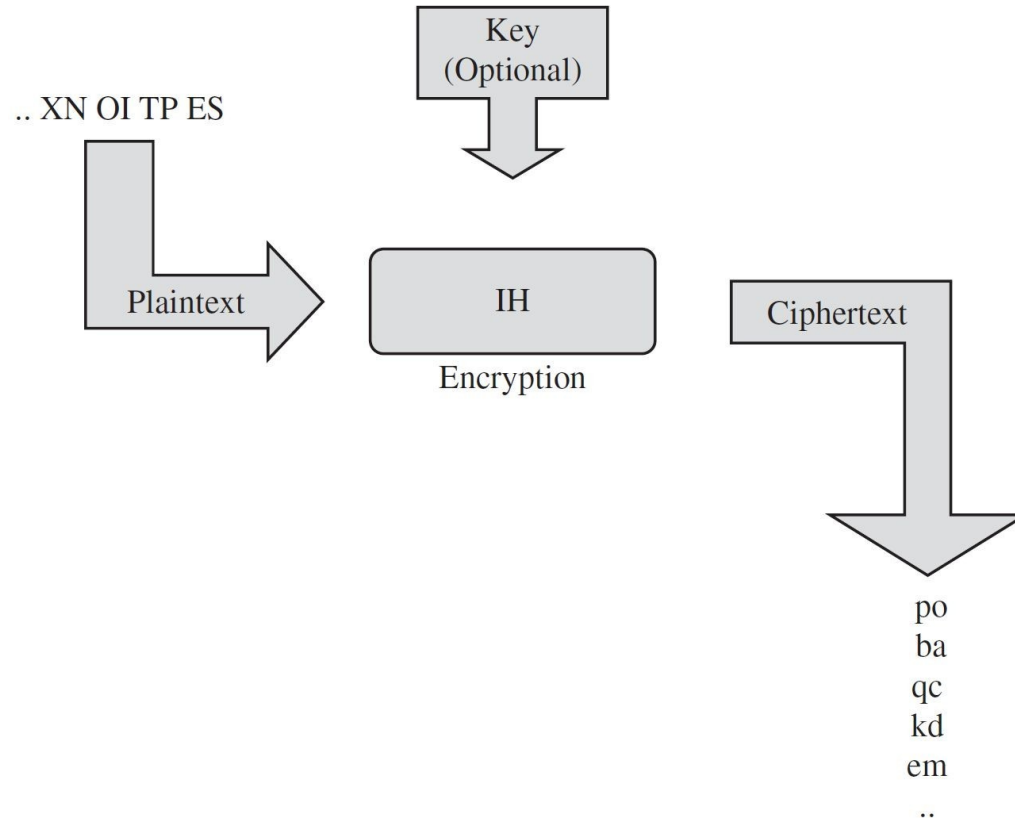


Stream ciphers encrypt one bit or one byte at a time.

BLOCK CIPHER

- A block cipher is a symmetric key cipher operating on fixed-length groups of bits, called blocks, with an unvarying transformation.
- A block cipher encryption algorithm might take (for example) a 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext.
- The exact transformation is controlled using a second input — the secret key.
- Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of ciphertext together with the secret key, and yields the original 128-bit block of plaintext.

BLOCK ENCRYPTION



Block ciphers encrypt a fixed number of bits as a single chunk.

STREAM VS. BLOCK ENCRYPTION

	Stream	Block
Advantages	• <i>Speed of transformation.</i> Because each symbol is encrypted without regard for any other plaintext symbols, each symbol can be encrypted as soon as it is read. Thus, the time to encrypt a symbol depends only on the encryption algorithm itself, not on the time it takes to receive more plaintext. • <i>Low error propagation.</i> Because each symbol is separately encoded, an error in the encryption process affects only that character.	• <i>High diffusion.</i> Information from the plaintext is diffused into several ciphertext symbols. One ciphertext block may depend on several plaintext letters. • <i>Immunity to insertion of symbol.</i> Because blocks of symbols are enciphered, it is impossible to insert a single symbol into one block. The length of the block would then be incorrect, and the decipherment would quickly reveal the insertion.
Disadvantages	• <i>Low diffusion.</i> Each symbol is separately enciphered. Therefore, all the information of that symbol is contained in one symbol of ciphertext. • <i>Susceptibility to malicious insertions and modifications.</i> Because each symbol is separately enciphered, an active interceptor who has broken the code can splice pieces of previous messages and transmit a spurious new message that may look authentic.	• <i>Slowness of encryption.</i> The person or machine doing the block ciphering must wait until an entire block of plaintext symbols has been received before starting the encryption process. • <i>Padding.</i> A final short block must be filled with irrelevant data to make a full-sized block. • <i>Error propagation.</i> An error will affect the transformation of all other characters in the same block.

Shannon Substitution-Permutation Ciphers

- In 1949, Shannon introduced idea of **substitution-permutation (S-P) networks**
 - modern substitution-transposition product cipher
- These form the basis of **modern** block ciphers
- S-P networks are based on the two primitive cryptographic operations:
 - ***substitution (S-box)***
 - ***permutation (P-box) (transposition)***
- He also introduced the ideas of *confusion* and *diffusion*

Diffusion and Confusion

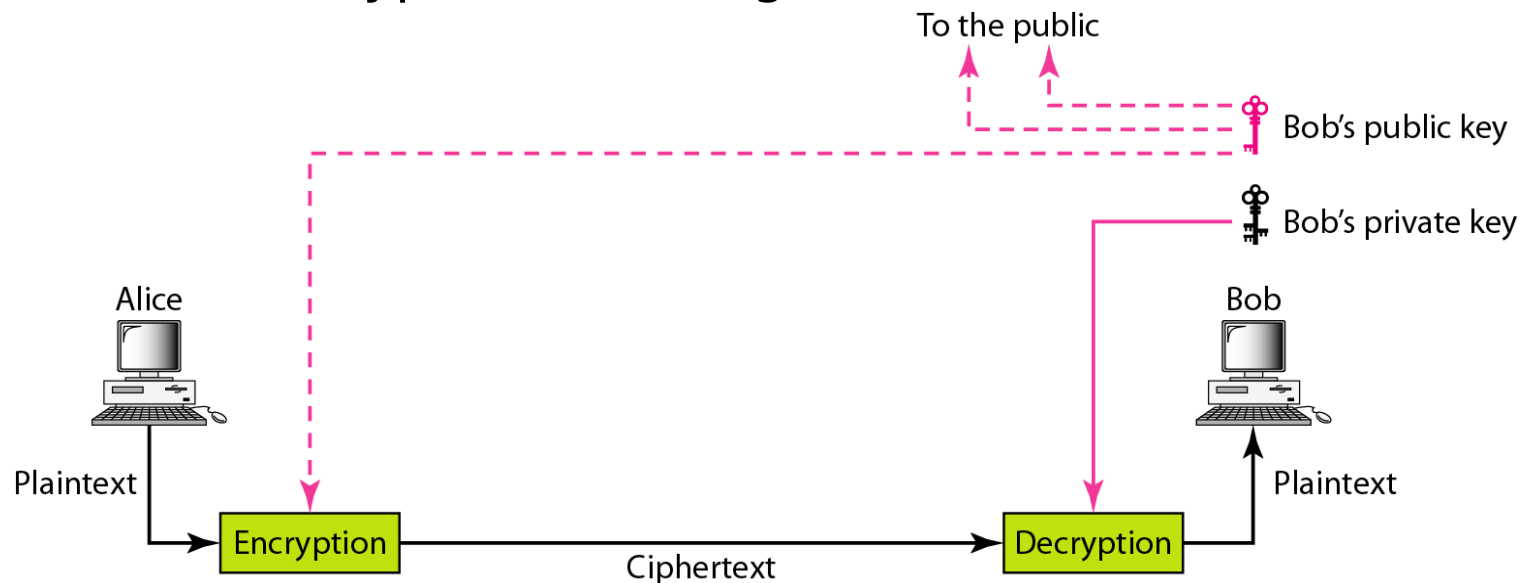
- Introduced by Claude Shannon **to thwart cryptanalysis based on statistical analysis**
 - Assume the attacker has some knowledge of the statistical characteristics of the plaintext
- Cipher needs to completely obscure statistical properties of original message
- More practically Shannon suggested combining elements to obtain:
 - **diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext
 - **confusion** – makes relationship between ciphertext and key as complex as possible

SHANNON'S CHARACTERISTICS OF "GOOD" CIPHERS

1. The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
2. The set of keys and the enciphering algorithm should be free from complexity.
3. The implementation of the process should be as simple as possible.
4. Errors in ciphering should not propagate and cause corruption of further information in the message.
5. The size of the enciphered text should be no larger than the text of the original message.

Asymmetric-key cryptography

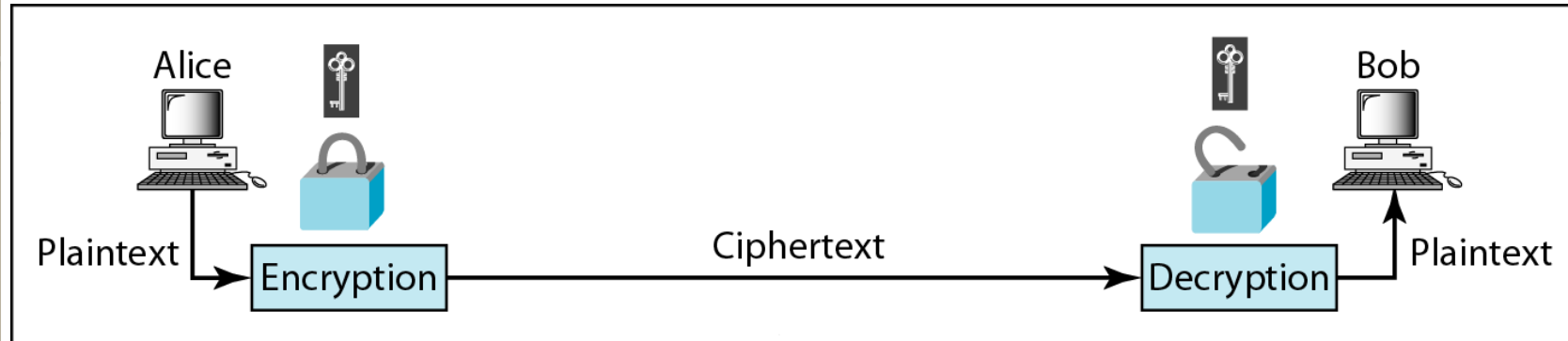
- In asymmetric or public-key cryptography, there are two keys: a private key and a public key.
- The private key is kept by the receiver & the public key is announced to the public.
- In Figure, imagine Alice wants to send a message to Bob.
- Alice uses the public key to encrypt the message.
- When the message is received by Bob, the private key is used to decrypt the message.



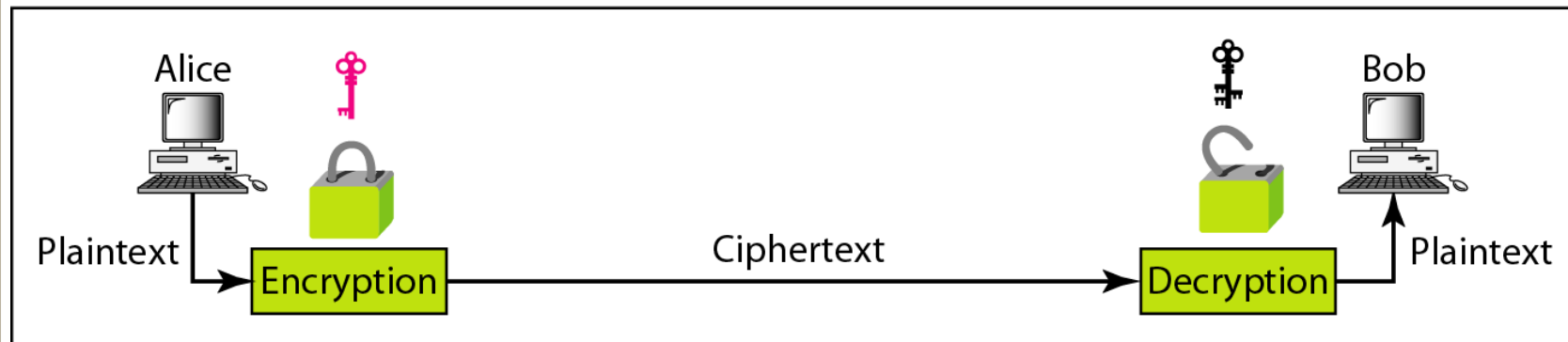
Comparison between two categories of cryptography

- Let us compare symmetric-key and asymmetric-key cryptography.
- **Encryption** can be thought of as electronic locking; **decryption** as electronic unlocking.
- The sender puts the message in a box and locks the box by using a key; the receiver unlocks the box with a key and takes out the message.
- The difference lies in the mechanism of the locking and unlocking and the type of keys used.
- In **symmetric-key** cryptography, the **same** key locks and unlocks the box.
- In **asymmetric-key** cryptography, one key locks the box, but another key is needed to unlock it.

Comparison...



a. Symmetric-key cryptography



b. Asymmetric-key cryptography

DES: THE DATA ENCRYPTION STANDARD

- The DES algorithm was developed in the 1970s by IBM for the U.S. National Institute of Standards and Technology (NIST)
- DES encrypts 64-bit blocks by using a 56-bit key.
- Double DES: Take two keys, k_1 and k_2 , and perform two encryptions, one on top of the other: $C = E(k_2, E(k_1, m))$
- Triple DES: $C = E(k_3, E(k_2, E(k_1, m)))$.

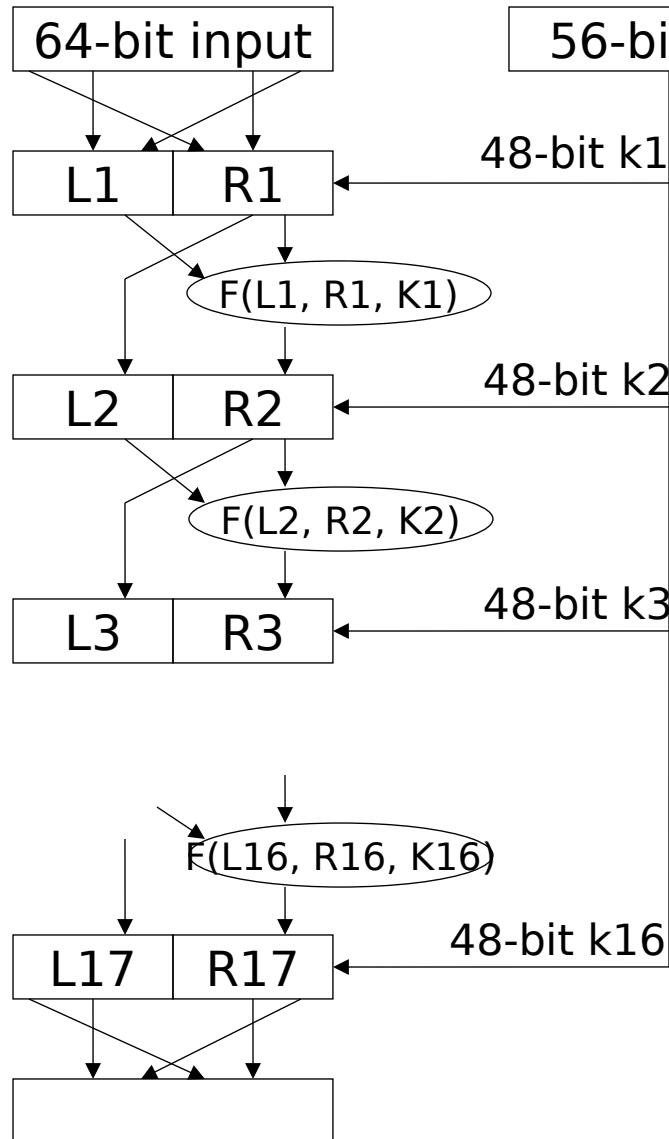
DES: THE DATA ENCRYPTION STANDARD

- DES is a block Cipher Algorithm
 - Encodes plaintext in 64 bit chunks. One parity bit for each of the 8 bytes thus it reduces to 56 bit

The algorithm process breaks down into the following steps:

1. The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
2. The initial permutation (IP) is then performed on the plain text.
3. Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
4. Each LPT and RPT goes through 16 rounds of the encryption process.
5. Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.
6. The result of this process produces the desired 64-bit ciphertext.

Data Encryption Standard (DES) Basics



DES run in reverse to
decrypt

Cracking DES

1997: 140 days

1999: 14 hours

TripleDES uses DES 3
times in tandem

Output from 1 DES is
input to next DES

FORMS OF DES

Form	Operation	Properties	Strength
DES	Encrypt with one key	56-bit key	Inadequate for high-security applications by today's computing capabilities
Double DES	Encrypt with first key; then encrypt result with second key	Two 56-bit keys	Only doubles strength of 56-bit key version
Two-key triple DES	Encrypt with first key, then encrypt (or decrypt) result with second key, then encrypt result with first key (E-D-E)	Two 56-bit keys	Gives strength equivalent to about 80-bit key (about 16 million times as strong as 56-bit version)
Three-key triple DES	Encrypt with first key, then encrypt or decrypt result with second key, then encrypt result with third key (E-E-E)	Three 56-bit keys	Gives strength equivalent to about 112-bit key about 72 quintillion (72×10^{15}) times as strong as 56-bit version

Modes of Operation

Experts using DES have five different modes of operation to choose from.

- Electronic Codebook (ECB). Each 64-bit block is encrypted and decrypted independently
- Cipher Block Chaining (CBC). Each 64-bit block depends on the previous one and uses an Initialization Vector (IV)
- Cipher Feedback (CFB). The preceding ciphertext becomes the input for the encryption algorithm, producing pseudorandom output, which in turn is XORed with plaintext, building the next ciphertext unit
- Output Feedback (OFB). Much like CFB, except that the encryption algorithm input is the output from the preceding DES
- Counter (CTR). Each plaintext block is XORed with an encrypted counter. The counter is then incremented for each subsequent block

AES: The Advanced Encryption Standard

- AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
- AES was introduced to replace DES, as DES uses very small cipher key and the algorithm was quite slower.

AES: The Advanced Encryption Standard

- The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES).
- It is found at least six times faster than triple DES.
- A replacement for DES was needed as its key size was too small.
- With increasing computing power, it was considered vulnerable against exhaustive key search attack.

AES: The Advanced Encryption Standard

- Triple DES was designed to overcome this drawback but it was found slow.

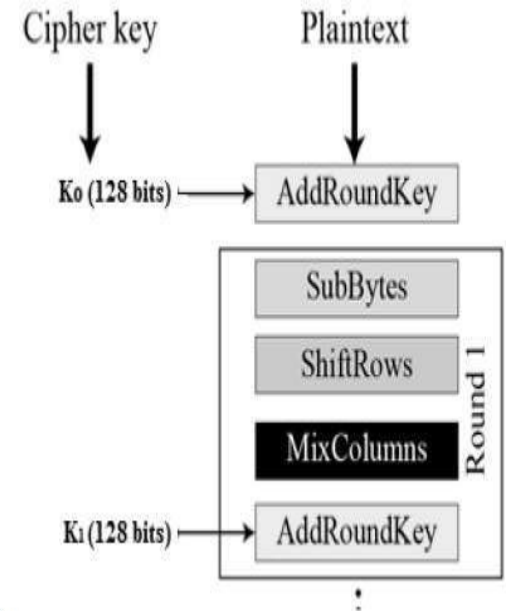
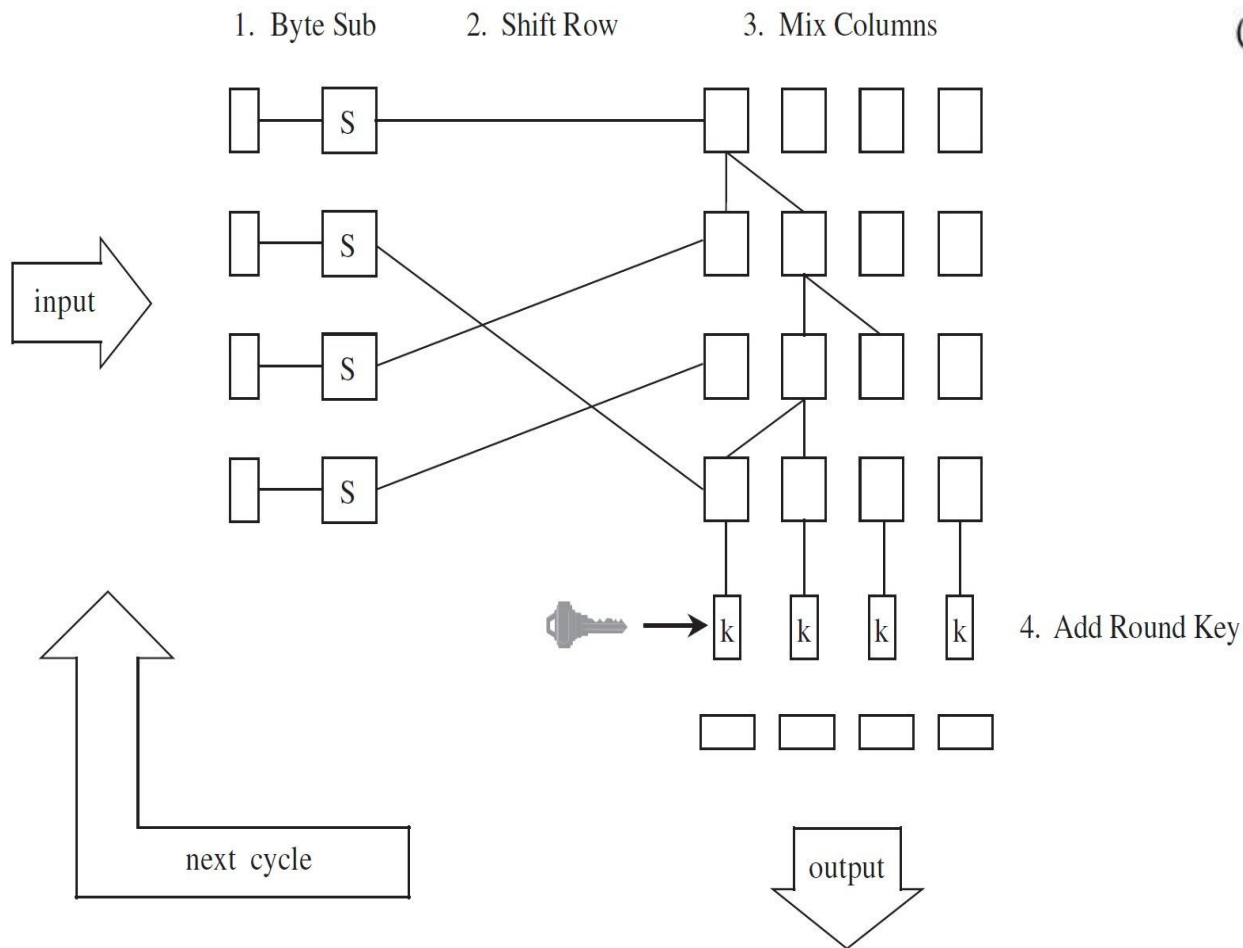
The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

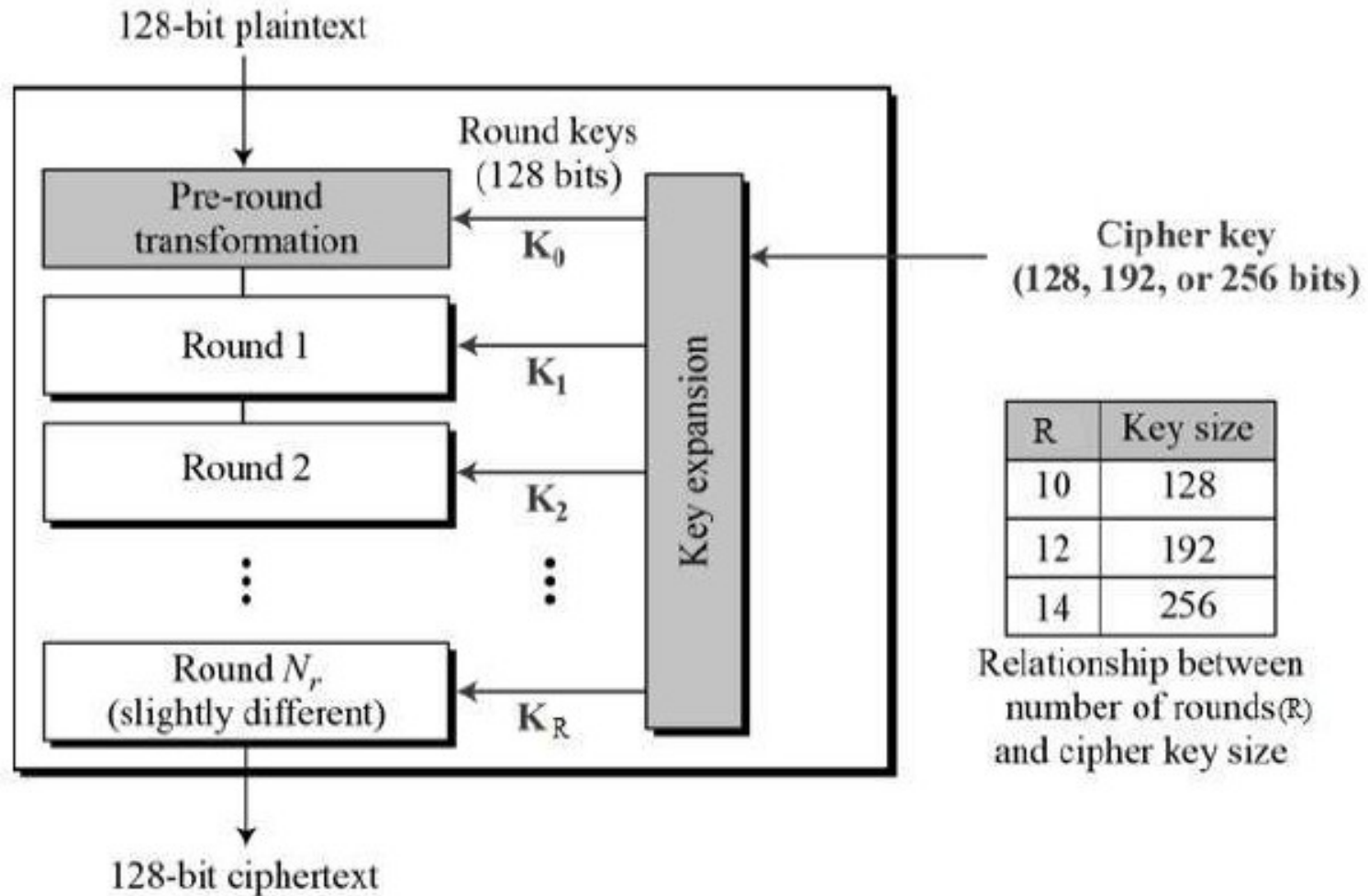
Operation of AES

- AES is an iterative rather than Feistel cipher.
- It is based on 'substitution-permutation network'.
- It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).
- Interestingly, AES performs all its computations on bytes rather than bits.
- Hence, AES treats the 128 bits of a plaintext block as 16 bytes.
- These 16 bytes are arranged in four columns and four rows for processing as a matrix
- Unlike DES, the number of rounds in AES is variable and depends on the length of the key.
- AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

STRUCTURE OF AES



STRUCTURE OF AES



DES VS. AES

	DES	AES
Developed	1977	2000
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128 bits
Security	Proven inadequate	Considered secure

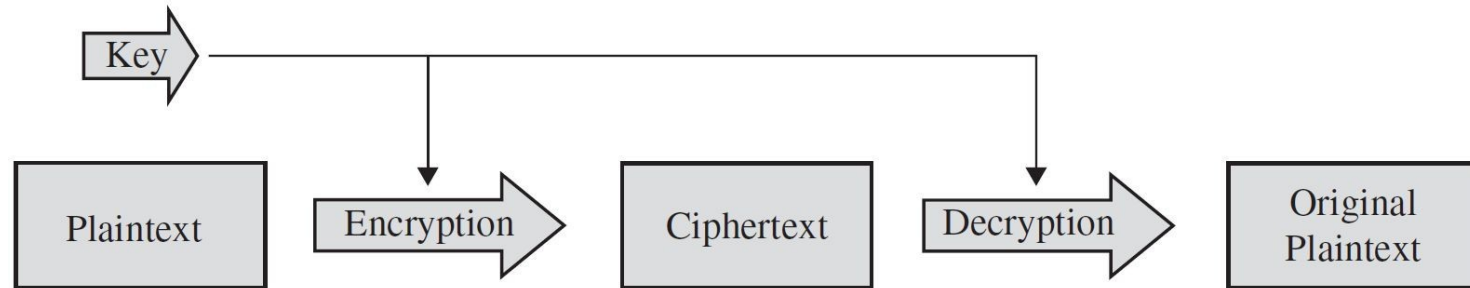
SYMMETRIC CRYPTOGRAPHY ALGORITHMS

- RC2,3,4,5,6
- CAST
- SAFER
- Twofish

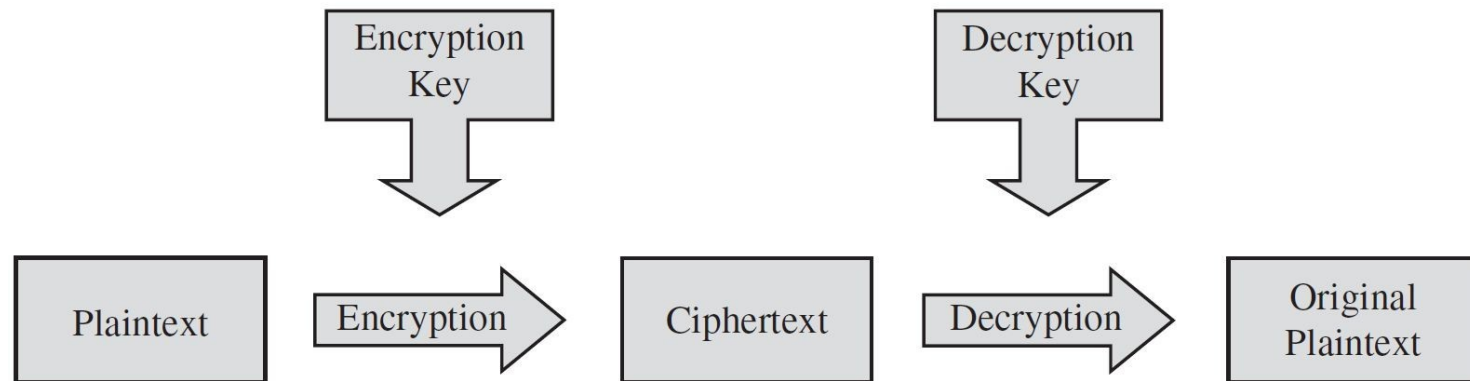
PROBLEM WITH SYMMETRIC KEY CRYPTOGRAPHY

- Large number of keys: If there are n people communicating with each other, we would need to distribute $n(n-1)/2$ symmetric keys between them. Is there some way to reduce the number of keys that need to be shared?
- For a digital signature: for instance, how can Alice prove that a message indeed came from Bob? This is important if both sides do not really trust one another, and Alice later disclaims that she didn't send any message to Bob.
- Security of exchange keys.
- **Solution: public key encryption**

SYMMETRIC AND ASYMMETRIC ENCRYPTION



(a) Symmetric Cryptosystem



(b) Asymmetric Cryptosystem

ASYMMETRIC CRYPTOGRAPHY / PUBLIC-KEY CRYPTOGRAPHY (1)

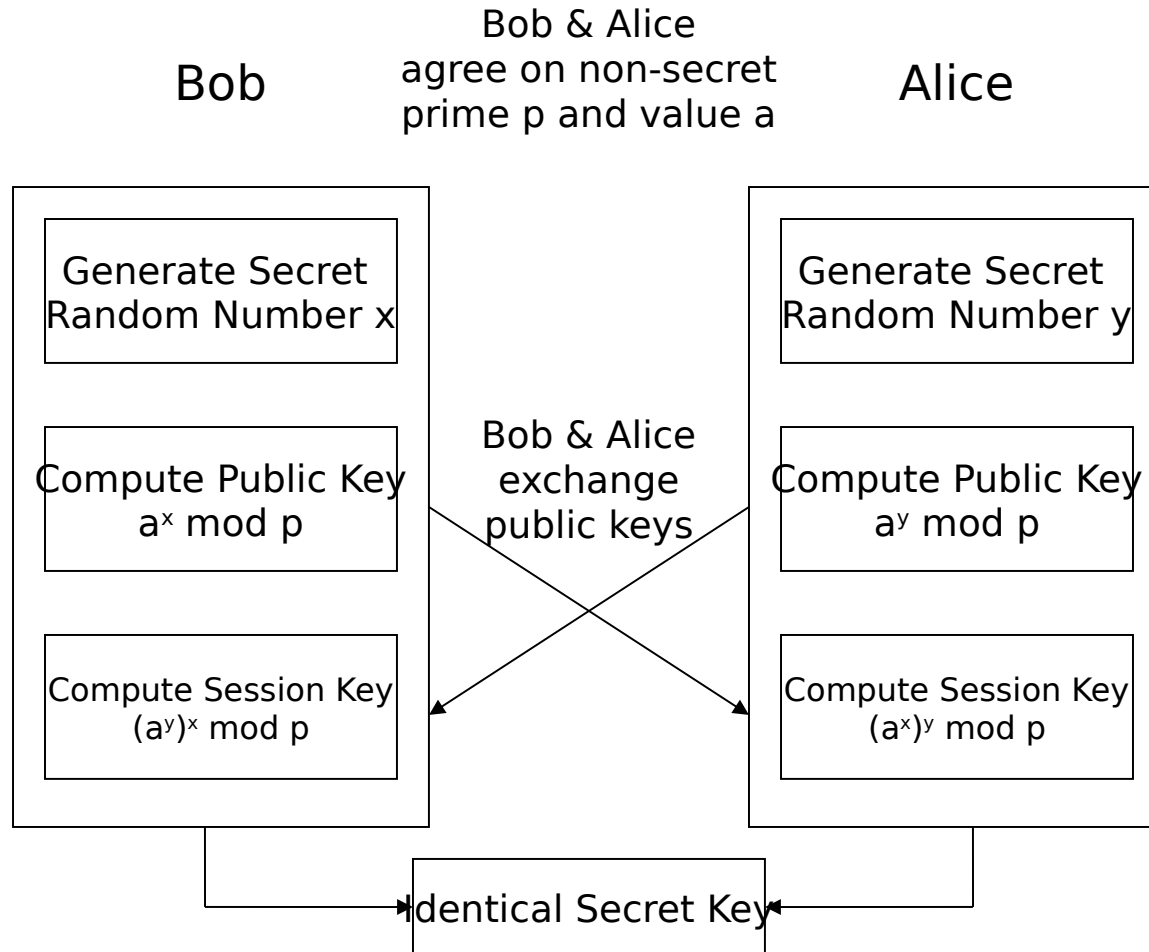
- Public-key cryptography, also known as asymmetric cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is secret (or private) and one of which is public.
- Although different, the two parts of this key pair are mathematically linked.
- The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt ciphertext or to create a digital signature.
- Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.
- Authors (Whitfield Diffie and Martin Hellman) of public-key cryptography received Turing Award in 2015: <http://amturing.acm.org/index.cfm>

A PUBLIC KEY ENCRYPTION SCHEME HAS 5 MAJOR PARTS

1. Plaintext - message to be encrypted.
2. Encryption Algorithm - it performs substitutions and transformations to the plaintext.
3. Public and Private Keys - a pair of keys, one for encryption and the other for decryption.
4. Ciphertext - this is the encrypted or scrambled message
5. Decryption Algorithm - it generates the ciphertext and the matching key to produce the plaintext.

- $P = D(k_{PRIV}, E(k_{PUB}, P)), P = D(k_{PUB}, E(k_{PRIV}, P))$
- $P = E(D(P)) = D(E(P))$

Key Diffie-Hellman Mathematical Analysis



Key Agreement cont..

- Diffie-Hellman is the first key agreement algorithm
Invented by Whitfield Diffie & Martin Hellman
 - Provided ability for messages to be exchanged securely without having to have shared some secret information previously
 - Inception of public key cryptography which allowed keys to be exchanged in the open
- No exchange of secret keys
 - Man-in-the middle attack avoided

COMPARISON BETWEEN SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY

Symmetric Cryptography	Asymmetric (Public key) Cryptography
Same key used to encrypt and decrypt	Different keys (public key and private key) used to encrypt and decrypt
Faster	Slower, typically by a factor of up to 10,000 times slower than symmetric algorithms
Need a secure channel to transfer the key	Needn't a security channel to transfer the key
Used when performance is required	Used to exchange key, encrypt communication, protect symmetric keys, authentication, signing

THE RSA ALGORITHM

- RSA (Designers: Ron Rivest, Adi Shamir, and Leonard Adleman, 1977) is one of the first practicable public-key cryptosystems and is widely used for secure data transmission.
- The RSA operates with arithmetic *mod n*, which makes factorization extremely difficult.
- The RSA cryptosystem is based on the assumption that **factorization of large integers is computationally hard**.
- This assumption is not known to be true, but is widely believed.
- It is not even known if factorization is an NP-complete problem.
- RSA keys are often of length a power of two, like 512, 1024, or 2048 bits.
- RSA authors received Turing Award in 2002.

THE RSA ALGORITHM

- Two keys, e and d , are used for decryption and encryption. They are actually interchangeable.
- n, e, d are produced from 2 prime numbers.
- The plaintext block m is encrypted as $m^e \bmod n = c$. Because the exponentiation is performed $\bmod n$, inferring from c to m is extremely difficult.
- However, the decrypting key d is carefully chosen so that $c^d \bmod n = m$. Thus, the legitimate receiver who knows d simply computes $c^d \bmod n = m$ and recovers m without having to factor n .

THE RSA ALGORITHM

Setup

1. To setup a public-private key pair, principal choose two primes p and q and keeps them secret, then computes $n = p * q$.
2. $\phi(n) = \phi(p * q) = \phi(p)\phi(q) = (p-1)*(q-1)$
3. Choose e , $\gcd(e, \phi(n)) = 1$, and $e < \phi(n)$. (e can be small; often 3, 17, or 65537 are chosen)
4. Select d , where $(d * e) \bmod \phi(n) = 1$.
5. public key is (e, n) and the private key is (d, n)

Operation

1. encryption of plaintext m : compute $c = m^e \bmod n$
2. decryption of ciphertext c : compute $m = c^d \bmod n$

Example

e:

1. Setup: $p=61, q=53, n=p*q=61*53=3233$
2. $\phi(n) = (p-1)*(q-1) = (61-1)*(53-1) = 3120$,
3. Choose $e=17$, prime with 3120, $\gcd(e, 3120)=1$, and $e < 3120$,
4. Select $d=2753$, because $(2753*17) \bmod 3120 = 1$
5. public key is $(17, 3233)$, private key is $(2753, 3233)$

Operation

1. encryption:
 $m = 65, c = m^e \bmod n = 65^{17} \bmod 3233 = 2790$
2. decryption:
 $m = c^d \bmod n = 2790^{2753} \bmod 3233 = 65$

THE RSA ALGORITHM

- Choose two large prime numbers p & q
- Compute $n=pq$ and $z=(p-1)(q-1)$
- Choose number e , less than n , which has no common factor (other than 1) with z
- Find number d , such that $ed - 1$ is exactly divisible by z
- Keys are generated using n , d , e
 - o Public key is (n,e)
 - o Private key is (n, d)
- Encryption: $c = m^e \bmod n$
 - o m is plain text
 - o c is cipher text
- Decryption: $m = c^d \bmod n$
- Public key is shared and the private key is hidden

RSA

$P=5$ & $q=7$

$n=5*7=35$ and $z=(4)*(6) = 24$

$e = 5$

$d = 29$, $(29 \times 5 - 1)$ is exactly divisible by 24

Keys generated are

Public key: (35,5)

Private key is (35, 29)

Encrypt the word love using ($c = m^e \bmod n$)

Assume that the alphabets are between 1 & 26

Plain Text	Numeric Representation	m^e	Cipher Text ($c = m^e \bmod n$)
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

CLASSROOM EXAMPLE FOR RSA

Example:

1. $p=3, q=5, n=p*q=15$
2. $\varphi(n)=\varphi(15)=\varphi(3)\varphi(5)=(3-1)*(5-1)=8$
3. $e=7$, because $\gcd(7,8)=1$
4. $d=7$, because $(d*e) \bmod 8=1$
5. if $m=2$
6. $c=m^e \bmod n=2^7 \bmod 15=8$
7. $m=c^d \bmod n=8^7 \bmod 15=2$

Exercise:

$$p=3, q=11, m=2$$

HOMEWORK

$$p=11, q=13, m=3$$

1. create private key and public key
2. use the keys to demonstrate the encryption and decryption to m

ASYMMETRIC ALGORITHMS

- Diffie-Hellman
- RSA
- El Gamal
- Elliptic Curve Cryptography (ECC)

ASYMMETRIC ENCRYPTION TYPES

Two most popular algorithms are RSA & El Gamal

- RSA
 - o Developed by Ron Rivest, Adi Shamir, Len Adelman
 - o Both public and private key are interchangeable
 - o Variable Key Size (512, 1024, or 2048 bits)
 - o Most popular public key algorithm
- El Gamal
 - o Developed by Taher El-Gamal
 - o Variable key size (512 or 1024 bits)
 - o Less common than RSA, used in protocols like PGP

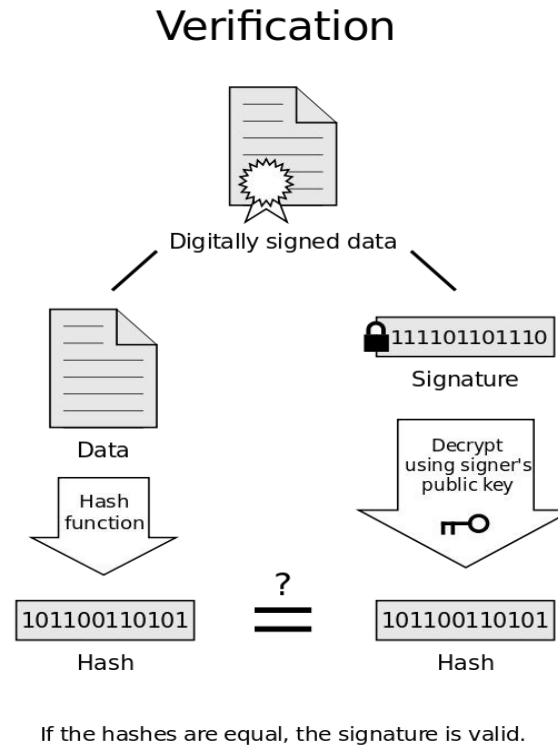
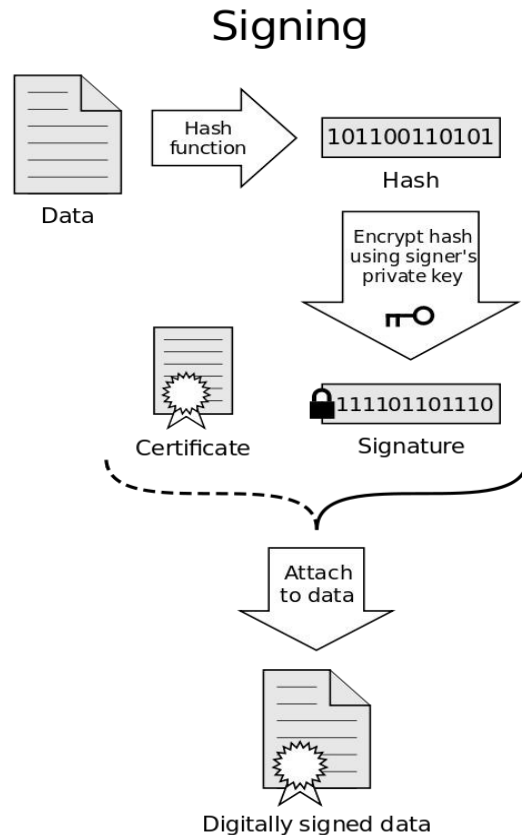
ENCRYPTION PROTOCOLS

- **Pretty Good Privacy (PGP)**
 - Used to encrypt e-mail using session key encryption
 - Combines RSA, Triple DES, and other algorithms
- **Secure/Multipurpose Internet Mail Extension (S/MIME)**
 - Newer algorithm for securing e-mail
 - Backed by Microsoft, RSA, AOL
- **Secure Socket Layer(SSL) and Transport Layer Socket(TLS)**
 - Used for securing TCP/IP Traffic
 - Mainly designed for web use
 - Can be used for any kind of internet traffic

DIGITAL SIGNATURE

- A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document.
- A valid digital signature gives a recipient reason to believe that the message was created by a trustable sender, such that the sender cannot deny having sent the message and that the message was not altered in integrity.
- Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

DIGITAL SIGNATURE



A diagram showing how a digital signature is applied and then verified.

DIGITAL SIGNATURE

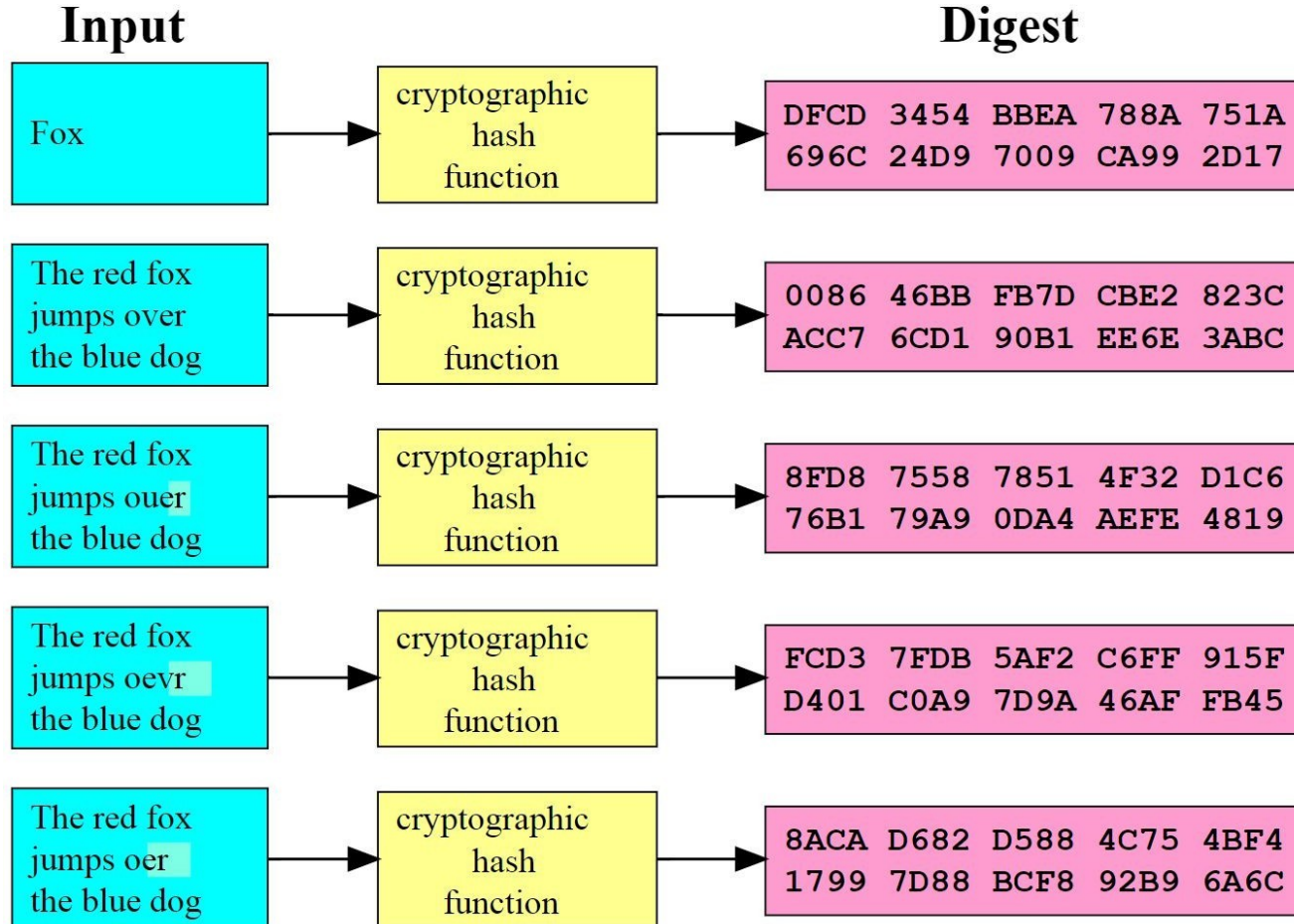
A digital signature consists of

1. a file
2. demonstration that the file has not been altered
3. indication of who applied the signature
4. validation that the signature is authentic, that it belongs to the signer
5. connection of the signature to the file

HASH FUNCTIONS

- Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key.
- A hash function, an output value deterministic will be created from an input value.
- For any input value, you will always receive the same output value whenever the hash function is run.
- It is impossible to recover the the contents or length of the plaintext from hash.
- Typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus.
- Are commonly employed by many operating systems to encrypt passwords.
- Provide a measure of the integrity of a file.

EXAMPLE OF HASH FUNCTION



HASHING ALGORITHMS

- MD5
 - Computes 128-bit hash value
 - Widely used for file integrity checking
- SHA-1
 - Computes 160-bit hash value
 - NIST approved message digest algorithm
- HAVAL
 - Computes between 128 and 256 bit hash
 - Between 3 and 5 rounds
- RIPEMD-160
 - Developed in Europe published in 1996
 - Patent-free

REFERENCES

- Alfred J. Menezes, Paul C. van Oorschot and Scott A., Handbook of Applied Cryptography, ISBN-13: 978-0849385230 □ CRC Press, 1996.
- Chapter 2, chapter 12, Charles P. Pfleeger, Security in Computing, Fifth Edition, Prentice Hall, ISBN-13: 978-0-13-408504-3, 2015.