# Encryption

SECURE COMMUNICATIONS & CRYPTOGRAPHY

Mark Cummins, Institute of Technology Blanchardstown

# Encryption

- Cryptography can be defined as the process of concealing the contents of a message from all except those who know the key.
- Encryption is the process used within cryptography to convert plaintext into cipher text
- Symmetric and asymmetric are the two primary types of encryptions
- Symmetric encryption uses a single key, whereas asymmetric uses two keys.

# Key Terms

- Algorithm: the set of rules or mathematical formula used to encrypt and decrypt data.
- Plaintext: Cleartext that is readable
- Ciphertext:Data is scrambled and unreadable
- Encryption: the transformation of data into an unreadable format

# Key Terms

- Cryptographic key: A key is a piece of information that controls how the cryptographic algorithm functions. It can be used to control the transformation of Plaintext to ciphertext or ciphertext to plaintext

- Symmetric Encryption: Uses the same key to encode and decode data

- Asymmetric Encryption: Uses different keys for encryption and decryption. Each participant is assigned a pair of keys, what one does the other undoes.

# Symmetric and Asymmetric Differences

**Symmetric**

- Faster than Asymmetric
- Difficult key distribution
- Only provides confidentiality

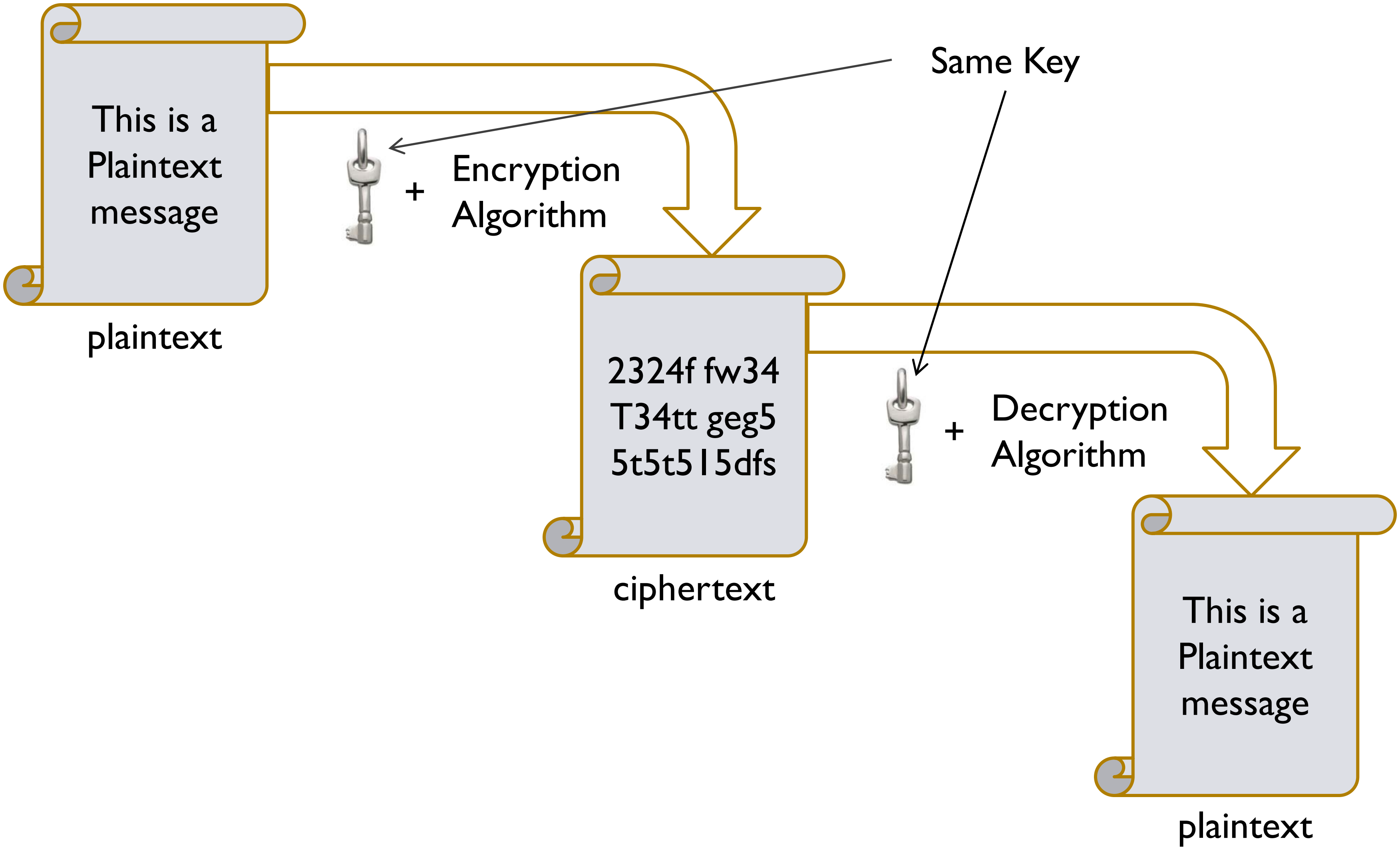
**Asymmetric**

- Slower than Symmetric
  (typically hundreds to thousands times slower)
- Easy key exchange
- Can provide confidentiality and authentication

# Symmetric Encryption

- Symmetric encryption is the older of the two forms of encryption.
- It uses a single shared secret key for encryption and decryption
- Symmetric-key algorithms can be divided into stream ciphers and block ciphers.
- Stream ciphers encrypt the bytes of the message one at a time, and block ciphers take a number of bytes and encrypt them as a single unit.

# Symmetric Encryption



# Symmetric Encryption

- Symmetric encryption is fast and is considered strong if large enough keys are used

- It does however have three big disadvantages
  - Key distribution:
    - We need a secure method to exchange keys
  - Key management:
    - We need a shared key for each pair of users
  - Authentication:
    - It doesn't offer us authentication

# Symmetric Algorithms

- DES - Data encryption standard (still most widely used)
- Blowfish - Intended as a DES replacement
- Rijndael - The current AES (Advanced encryption standard)
- RC4 - Rivest Cipher 4 (stream based)
- RC5 - Rivest Cipher 5
- SAFER - Secure and fast encryption routine

# Rivest Cipher (RC)

- RC is a general term for a family of ciphers designed by Ron Rivest (RC2, RC4, RC5,RC6)

- RC2:
  - Earliest algorithm in the series
  - 64-bit block cipher that can be used with DES
  - Variable key size

- RC4:
  - A stream cipher, which is faster than block mode ciphers
  - The 40-bit version was originally available in WEP
  - Most commonly found as 128 bit version

# Rivest Cipher (RC)

- RC5:
  - Block based cipher
  - Has a number of rounds (0-255)
  - Key size range (0 – 2040 bits)

- RC6:
  - Variable key sizes, and rounds
  - Two extra feature over RC5
    - Integer multiplication
    - Four 4-bit working registers

# Data Encryption Standard (DES)

- Developed by National Bureau of Standards (NBS)
  - Now known as NIST

- Originally based on IBM algorithm called Lucifer, it was dopted as the national standard in 1976

- DES had to be recertified every five years
  - In 1993 NIST states that DES was beginning to outlive its usefulness and started looking for a replacement (AES)

- In 1998 the Electronic Frontier Foundation (EFF) managed to crack DES in 23 hours.
  - They did however use 100,000 machines

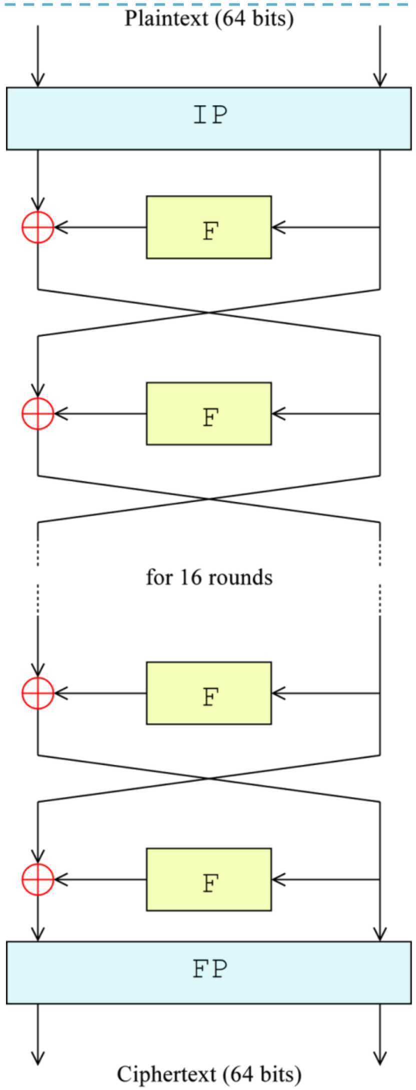
# Data Encryption Standard (DES)

- DES is a Block Cipher and processes plaintext blocks of 64-bits into ciphertext blocks of 64-bits
- It has a 64 bit key (56-bits are really only used)
- Because it's a symmetric algorithm it uses the same key to encrypt and decrypt
- DES performs 16 rounds
  - Each round takes the 64-bits and then uses a substitution cipher before performing a permutation on the input.

# Data Encryption Standard (DES)

- To extend the usefulness of DES, Triple DES or TDES was invented.
- It is much more secure as it has a key length of 168-bits (3 * 56-bit keys) but is three times as slow to implement
- Why no double DES?

# Data Encryption Standard (DES)




One round of the DES Cipher shown

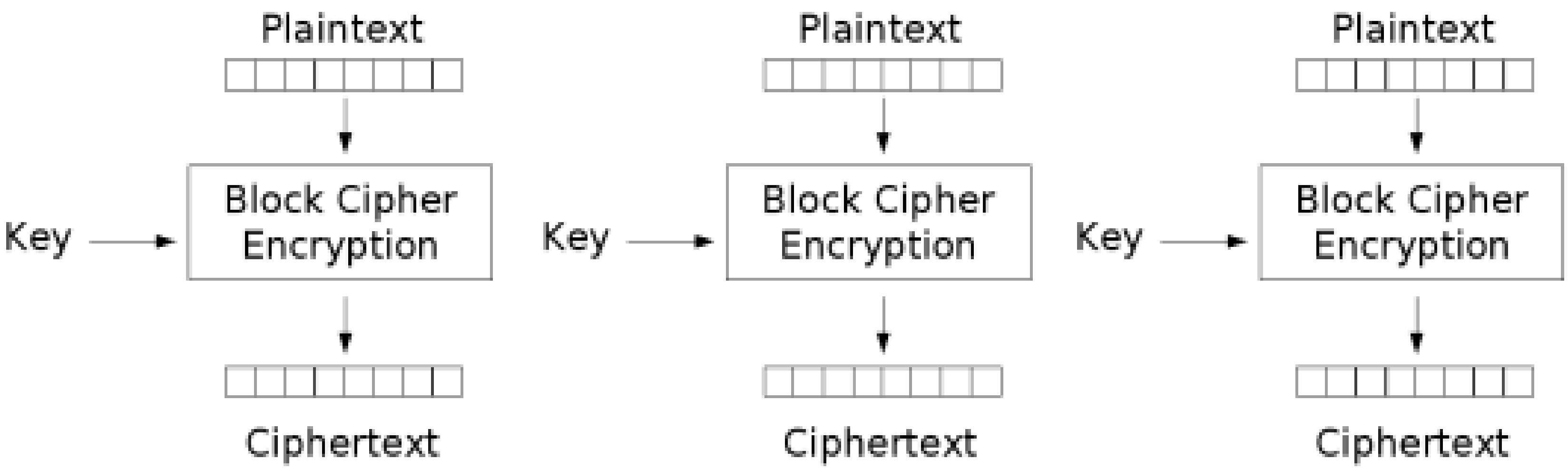
DES repeats this 16 times

# Block Cipher Modes

- There are four common modes or types
  - Electronic Code Book (ECB) mode
  - Cipher Block chaining (CBC) mode
  - Cipher Feedback (CFB) mode
  - Output Feedback (OFB) mode

# Block Cipher Modes

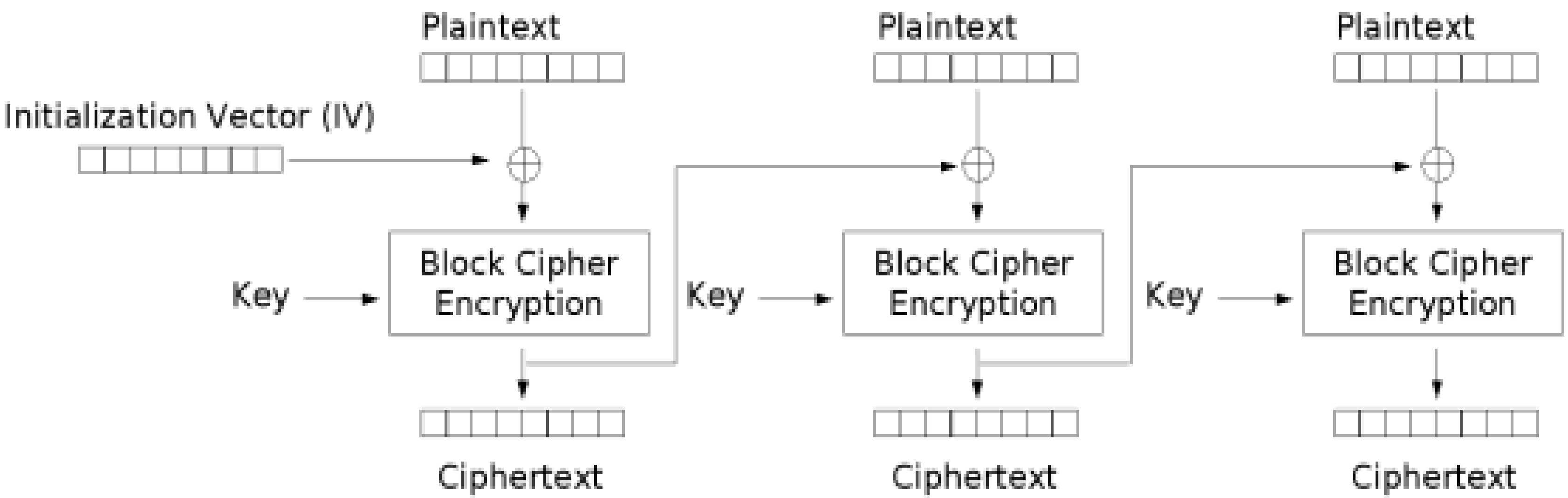
- Electronic Code Book (ECB) mode




Electronic Codebook (ECB) mode encryption

# Block Cipher Modes

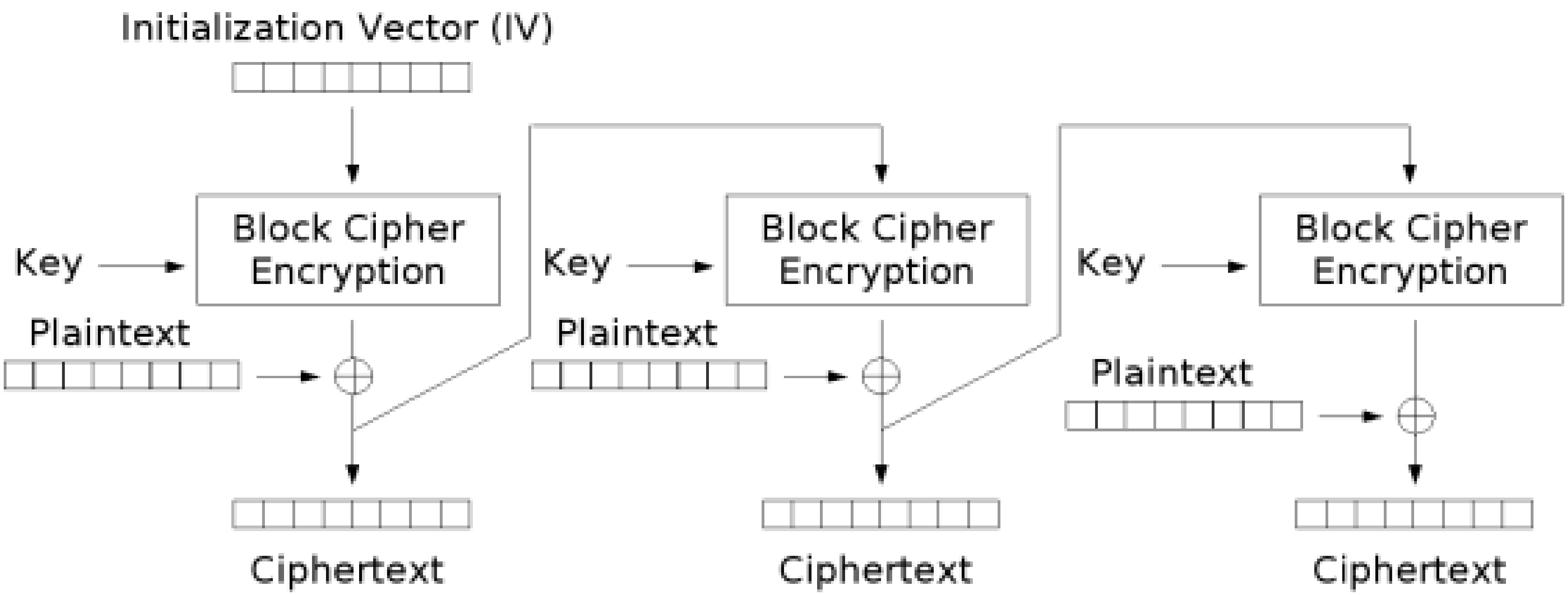
- Cipher Block chaining (CBC) mode




Cipher Block Chaining (CBC) mode encryption

# Block Cipher Modes

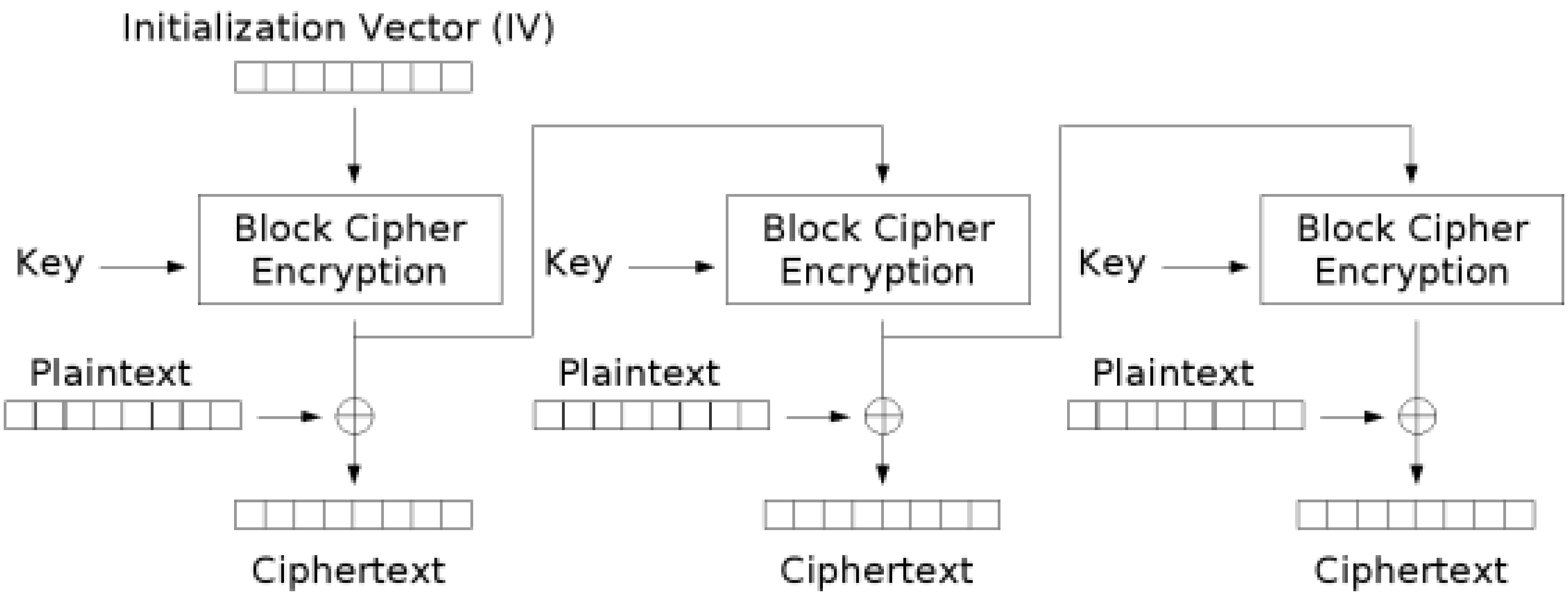
- Cipher Feedback (CFB) mode




Cipher Feedback (CFB) mode encryption

# Block Cipher Modes

- Output Feedback (OFB) mode




Output Feedback (OFB) mode encryption


Mark Cummins, Institute of Technology Blanchardstown

# Advanced Encryption Standard (AES)

- The Rijndael cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen
- Chosen in 2001 By NIST as the replacement for DES
- Supports a block size of 128 and variable key lengths of 128,192 or 256 bits
- It is considered a fast, simple and robust encryption mechanism

# Advanced Encryption Standard (AES)

- It uses four-step, parallel series of rounds
  - Byte sub:
    - Each byte is replaced by an S-box substation
  - Shift row:
    - Bytes are arranged in a rectangle and shifted
  - Mix column:
    - Matrix multiplication is performed based on the arranged rectangle
  - Add round key:
    - This rounds sub key is coded in

# Asymmetric Encryption (Aka. Public Key Cryptography)

- Unlike symmetric encryption, which uses a single shared key, asymmetric encryption uses two keys.

- They do not need a secure initial exchange as one of the keys can be made public, without any treats to the security.

- Asymmetric encryption techniques can also be used for digital signatures

# Asymmetric Encryption

- What one key does the second key undoes
- The keys are referred to as public and private keys
- The public key can be published and given to anyone, the user keeps the private key a secret
- Asymmetric encryption tends to use one way functions, but uses a trapdoor function within them to quickly reverse the operation

# Asymmetric Encryption

- An asymmetric-key cryptosystem was published in 1976 by Whitfield Diffie and Martin Hellman, disclosed a method of public-key agreement.
- This method of key exchange, which uses exponentiation in a finite field, came to be known as Diffie-Hellman key exchange.

# Asymmetric Encryption

- This was the first published practical method for establishing a shared secret-key over an authenticated (but not private) communications channel without using a prior shared secret.

# Asymmetric Encryption

- Common Asymmetric functions:
  - Diffie-Hellman
  - RSA
  - ECC
  - EL Gamal

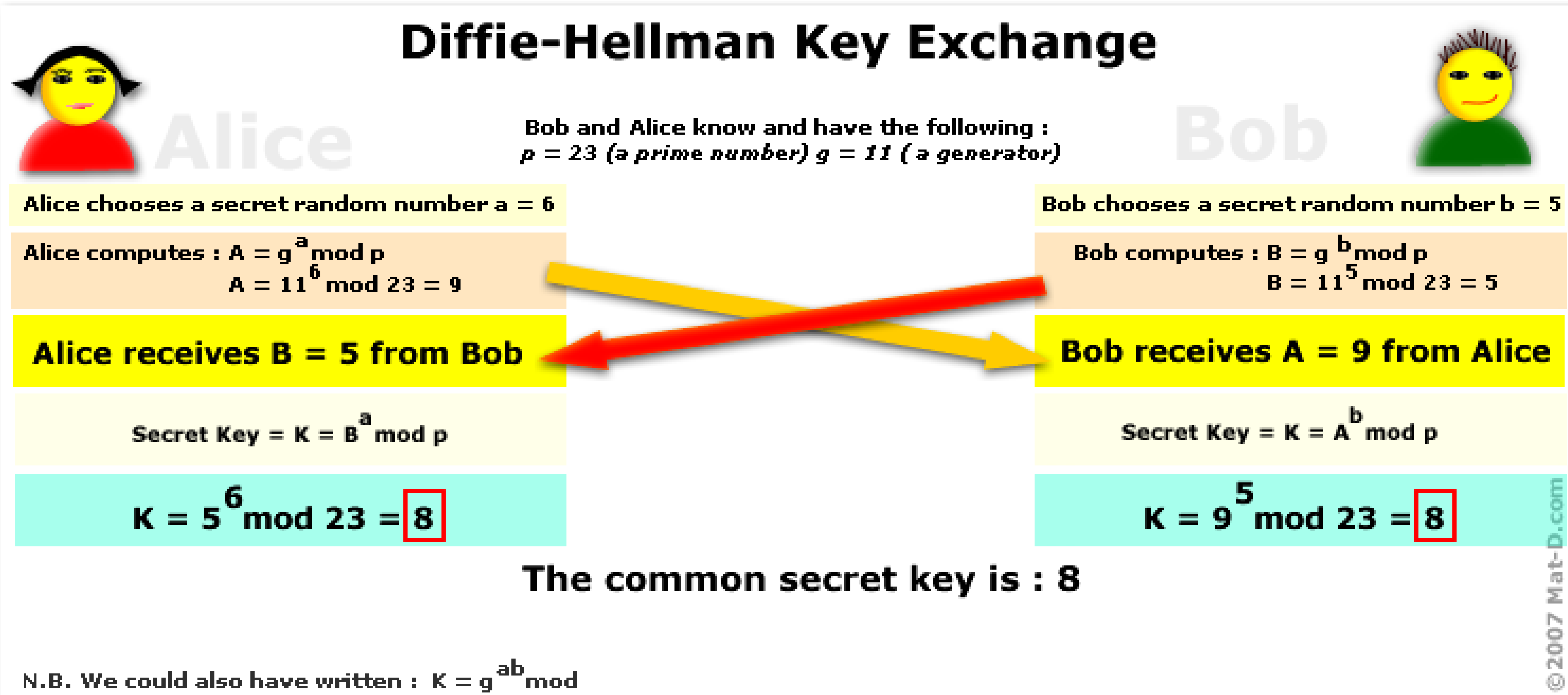
# Diffie-Hellman

- Was originally developed for use as a key exchange protocol
- It is used in SSL and IPSec
- It is vulnerable to man-in-the middle attacks
- This vulnerability can be overcome if you use digital signatures
- Based on the discrete logarithm problem

# Diffie-Hellman

- How it works
  - Alice and Bob must agree two numbers, these numbers can be sent to each other in public
    - p: some random prime number (the bigger the better)
    - g: a generator (A small prime number, usually 2,5, or 11)
  - Alice and Bob now each pick some secret number
    - a: the secret number picked by Alice
    - b: the secret number picked by Bob
  - Alice and Bob now work out $X = g^x \bmod p$ and send it to each other
    - Alice sends Bob $A = g^a \bmod p$
    - Bob sends Alice $B = g^b \bmod p$
  - Alice and Bob now compute their shared secret key
    - Alice computes $s = B^a \bmod p$
    - Bob computes $s = A^b \bmod p$

# Diffie-Hellman



# RSA

- Invented by Rivest, Shamir and Adleman in 1977
- Based on large number factorisation problem
- RSA key sizes can be very large (RFC 2537: does limited the size to 4096 bits)

# RSA

- How it works
  - Alice and Bob must agree two prime numbers, p and q
    - Alice and Bob now calculate $n = pq$
  - They now pick another prime number e
    - $e$ must be less than $(p-1)(q-1)$
  - Alice now send her public key (n,e) to Bob
  - Bob wanting to send a message M, to Alice, sends
    - $c = M^e \bmod n$

# RSA

- Alice recovers the message by calculating
  - $M = c^d \bmod n$
- We work out d as
  - $de = 1 \bmod (p-1)(q-1)$
- This works becuase
  - $c^d = M^{ed} \bmod n$

# RSA

- Let's take as an example
  - **p** = 7 and **q** = 3
- Now we are going to find **n**.
  - **n** = **p** x **q** = 7 x 3 = **21**
- Alice also needs to compute her private (or so called secret) key and the public key.
- In order to compute both keys we need to find **e** and **d** so that:
  - **e** x **d** mod **phi**(n) = 1.
- Let's take **e** = 7
- Now we need to find out **d** .
  - **7 d mod 12**.