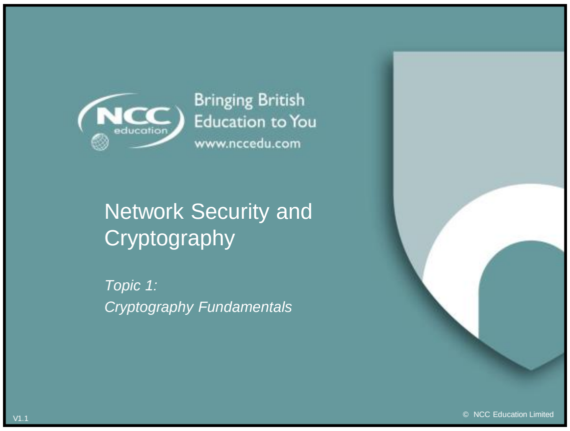
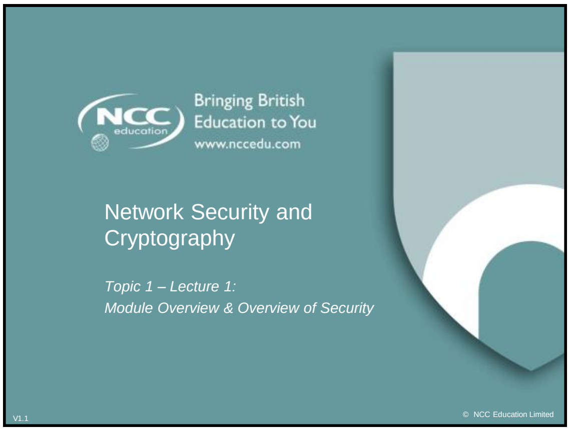


Bringing British Education to You
www.nccedu.com

Network Security and Cryptography

Topic 1:
Cryptography Fundamentals

V1.1 © NCC Education Limited

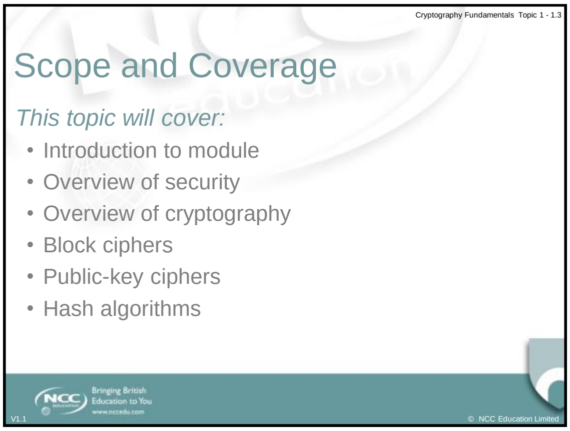


Bringing British Education to You
www.nccedu.com

Network Security and Cryptography

Topic 1 – Lecture 1:
Module Overview & Overview of Security

V1.1 © NCC Education Limited



Cryptography Fundamentals Topic 1 - 1.3

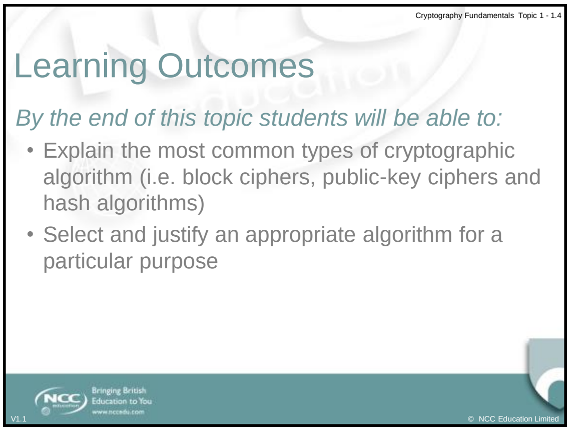
Scope and Coverage

This topic will cover:

- Introduction to module
- Overview of security
- Overview of cryptography
- Block ciphers
- Public-key ciphers
- Hash algorithms

Bringing British Education to You
www.nccedu.com

V1.1 © NCC Education Limited



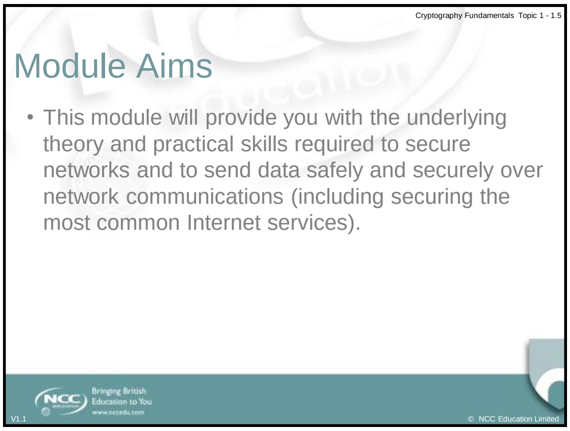
Cryptography Fundamentals Topic 1 - 1.4

Learning Outcomes

By the end of this topic students will be able to:

- Explain the most common types of cryptographic algorithm (i.e. block ciphers, public-key ciphers and hash algorithms)
- Select and justify an appropriate algorithm for a particular purpose

V1.1 © NCC Education Limited

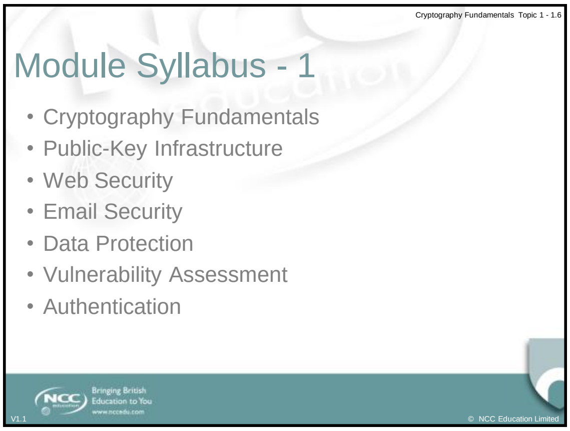


Cryptography Fundamentals Topic 1 - 1.5

Module Aims

- This module will provide you with the underlying theory and practical skills required to secure networks and to send data safely and securely over network communications (including securing the most common Internet services).

V1.1 © NCC Education Limited

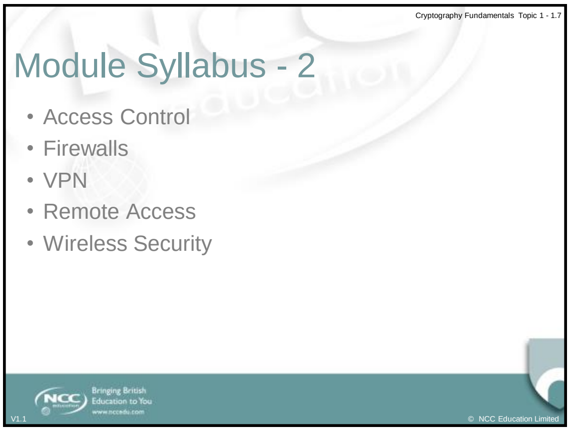


Cryptography Fundamentals Topic 1 - 1.6

Module Syllabus - 1

- Cryptography Fundamentals
- Public-Key Infrastructure
- Web Security
- Email Security
- Data Protection
- Vulnerability Assessment
- Authentication

V1.1 © NCC Education Limited

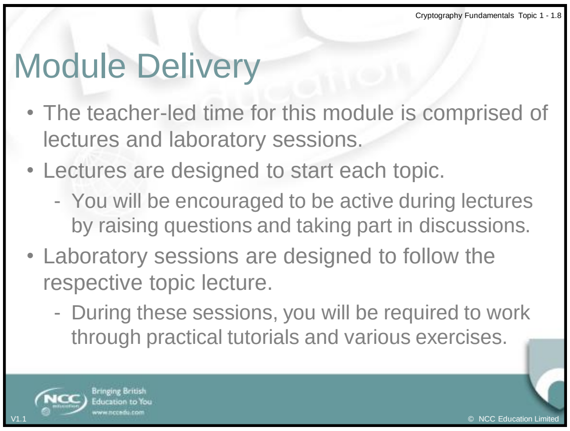


Cryptography Fundamentals Topic 1 - 1.7

Module Syllabus - 2

- Access Control
- Firewalls
- VPN
- Remote Access
- Wireless Security

V1.1 © NCC Education Limited

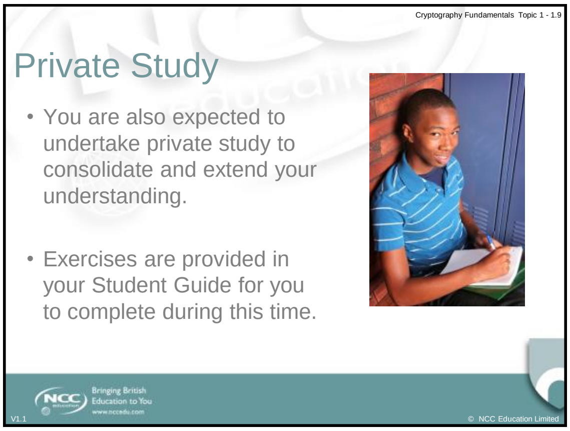


Cryptography Fundamentals Topic 1 - 1.8

Module Delivery

- The teacher-led time for this module is comprised of lectures and laboratory sessions.
- Lectures are designed to start each topic.
  - You will be encouraged to be active during lectures by raising questions and taking part in discussions.
- Laboratory sessions are designed to follow the respective topic lecture.
  - During these sessions, you will be required to work through practical tutorials and various exercises.

V1.1 © NCC Education Limited

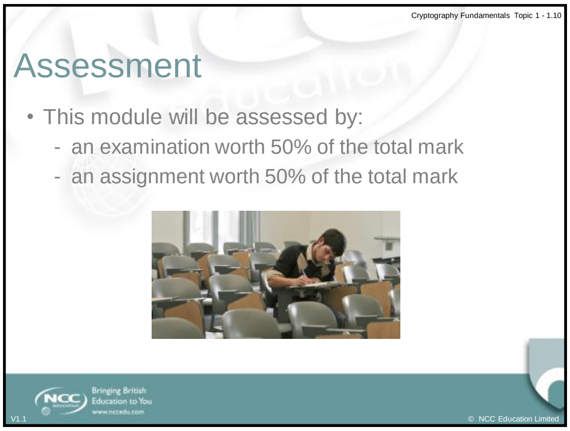


Cryptography Fundamentals Topic 1 - 1.9

Private Study

- You are also expected to undertake private study to consolidate and extend your understanding.
- Exercises are provided in your Student Guide for you to complete during this time.

V1.1 © NCC Education Limited



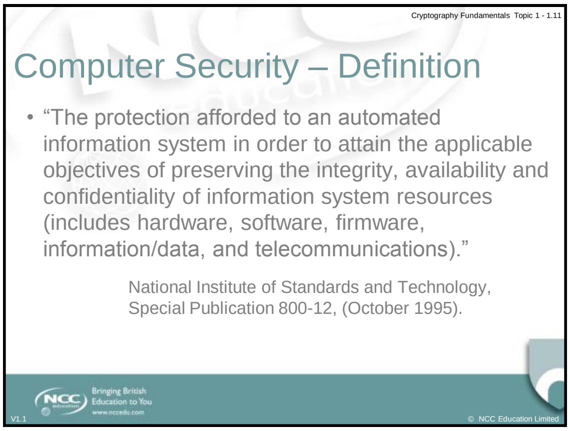
Cryptography Fundamentals Topic 1 - 1.10

Assessment

- This module will be assessed by:
  - an examination worth 50% of the total mark
  - an assignment worth 50% of the total mark

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



Cryptography Fundamentals Topic 1 - 1.11

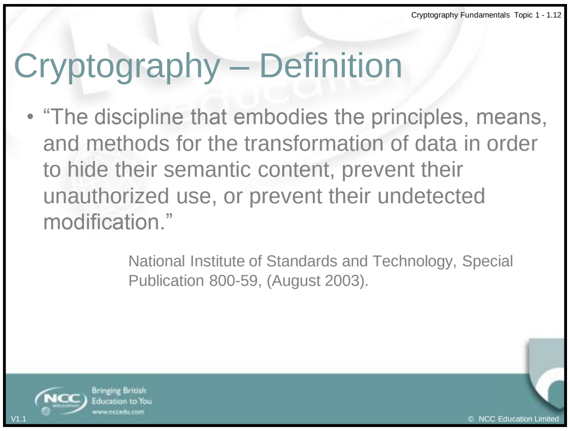
Computer Security – Definition

- “The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).”

  National Institute of Standards and Technology, Special Publication 800-12, (October 1995).

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



Cryptography Fundamentals Topic 1 - 1.12

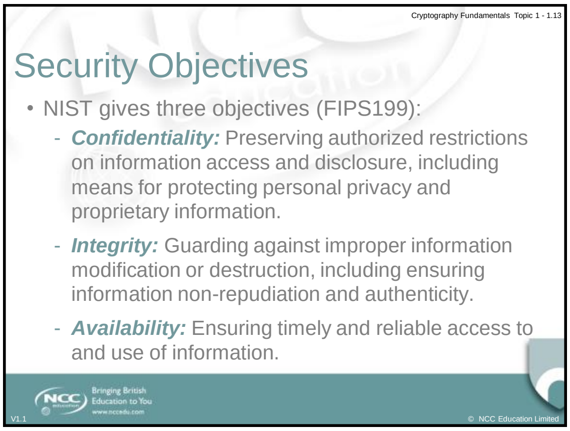
Cryptography – Definition

- “The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.”

  National Institute of Standards and Technology, Special Publication 800-59, (August 2003).

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



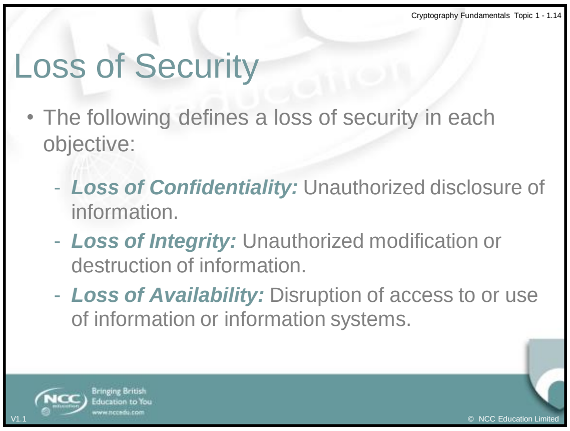
Cryptography Fundamentals Topic 1 - 1.13

Security Objectives

- NIST gives three objectives (FIPS199):
  - ***Confidentiality:*** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
  - ***Integrity:*** Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.
  - ***Availability:*** Ensuring timely and reliable access to and use of information.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



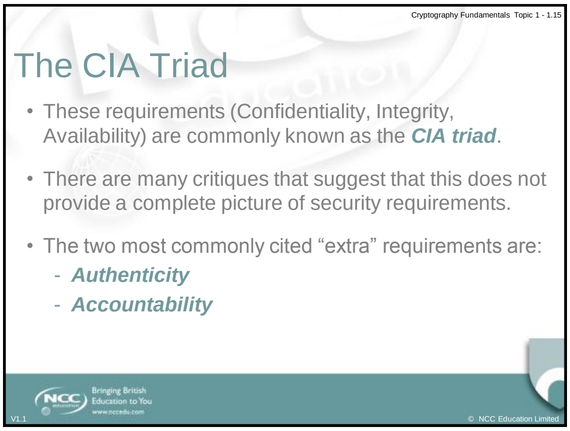
Cryptography Fundamentals Topic 1 - 1.14

Loss of Security

- The following defines a loss of security in each objective:
  - ***Loss of Confidentiality:*** Unauthorized disclosure of information.
  - ***Loss of Integrity:*** Unauthorized modification or destruction of information.
  - ***Loss of Availability:*** Disruption of access to or use of information or information systems.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



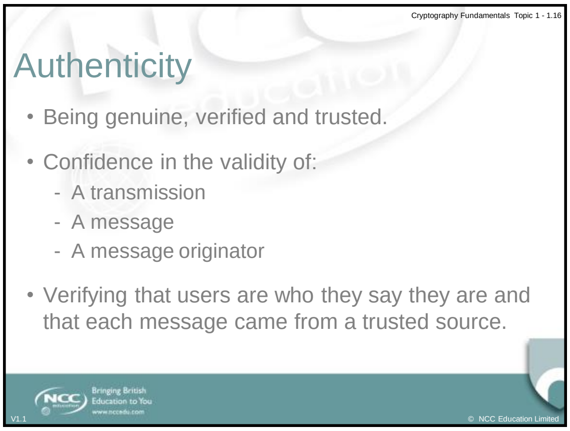
Cryptography Fundamentals Topic 1 - 1.15

The CIA Triad

- These requirements (Confidentiality, Integrity, Availability) are commonly known as the ***CIA triad***.
- There are many critiques that suggest that this does not provide a complete picture of security requirements.
- The two most commonly cited “extra” requirements are:
  - ***Authenticity***
  - ***Accountability***

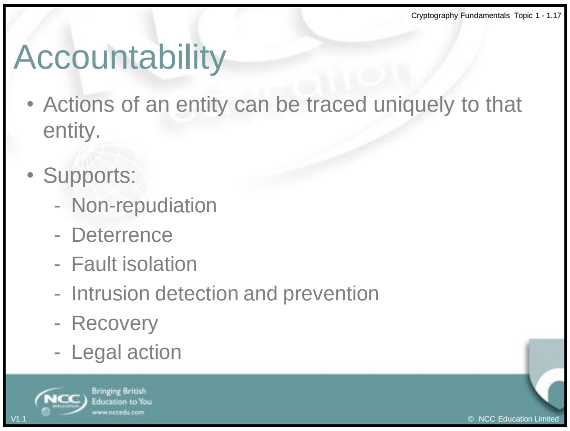
Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



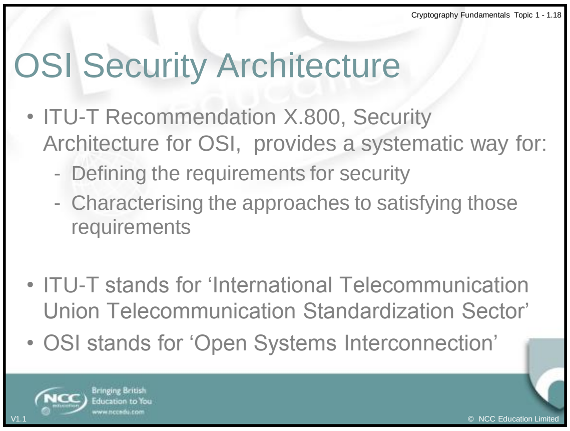
Authenticity

- Being genuine, verified and trusted.
- Confidence in the validity of:
  - A transmission
  - A message
  - A message originator
- Verifying that users are who they say they are and that each message came from a trusted source.



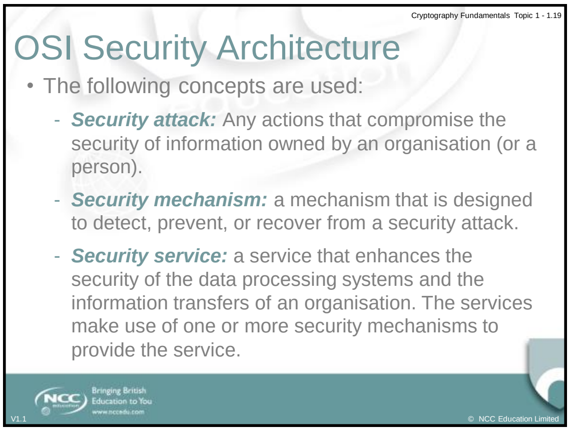
Accountability

- Actions of an entity can be traced uniquely to that entity.
- Supports:
  - Non-repudiation
  - Deterrence
  - Fault isolation
  - Intrusion detection and prevention
  - Recovery
  - Legal action



OSI Security Architecture

- ITU-T Recommendation X.800, Security Architecture for OSI, provides a systematic way for:
  - Defining the requirements for security
  - Characterising the approaches to satisfying those requirements
- ITU-T stands for ‘International Telecommunication Union Telecommunication Standardization Sector’
- OSI stands for ‘Open Systems Interconnection’



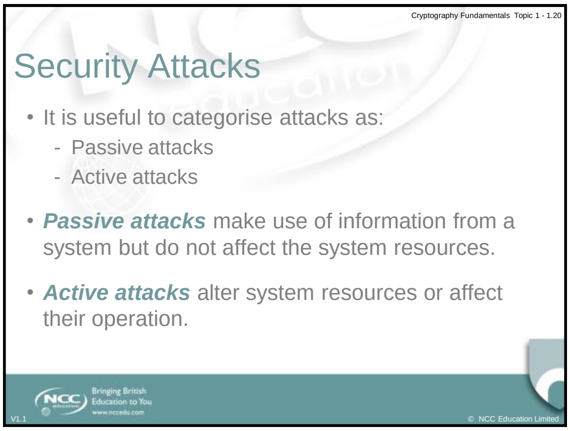
Cryptography Fundamentals Topic 1 - 1.19

OSI Security Architecture

- The following concepts are used:
  - ***Security attack:*** Any actions that compromise the security of information owned by an organisation (or a person).
  - ***Security mechanism:*** a mechanism that is designed to detect, prevent, or recover from a security attack.
  - ***Security service:*** a service that enhances the security of the data processing systems and the information transfers of an organisation. The services make use of one or more security mechanisms to provide the service.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



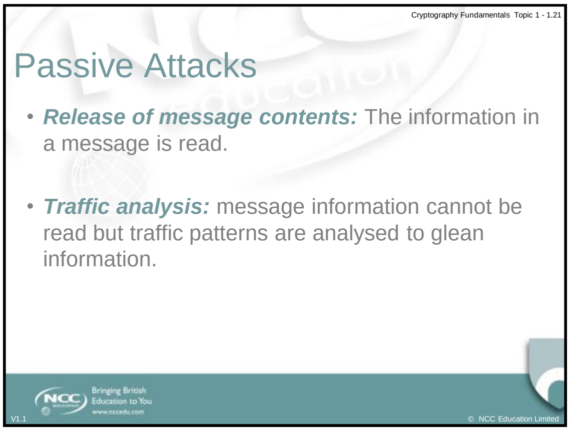
Cryptography Fundamentals Topic 1 - 1.20

Security Attacks

- It is useful to categorise attacks as:
  - Passive attacks
  - Active attacks
- ***Passive attacks*** make use of information from a system but do not affect the system resources.
- ***Active attacks*** alter system resources or affect their operation.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



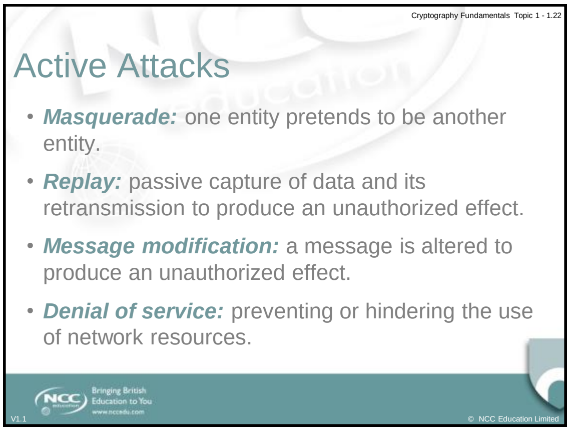
Cryptography Fundamentals Topic 1 - 1.21

Passive Attacks

- ***Release of message contents:*** The information in a message is read.
- ***Traffic analysis:*** message information cannot be read but traffic patterns are analysed to glean information.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



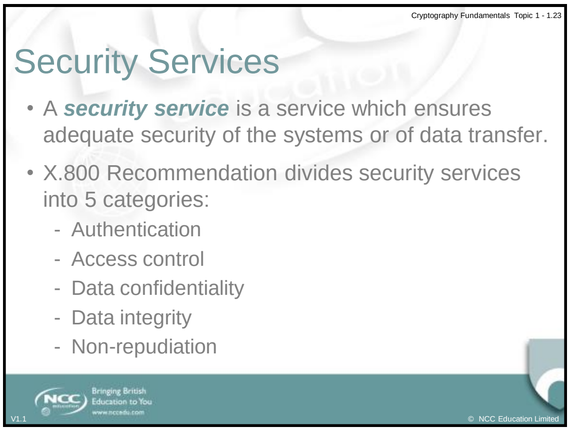
Cryptography Fundamentals Topic 1 - 1.22

Active Attacks

- ***Masquerade:*** one entity pretends to be another entity.
- ***Replay:*** passive capture of data and its retransmission to produce an unauthorized effect.
- ***Message modification:*** a message is altered to produce an unauthorized effect.
- ***Denial of service:*** preventing or hindering the use of network resources.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



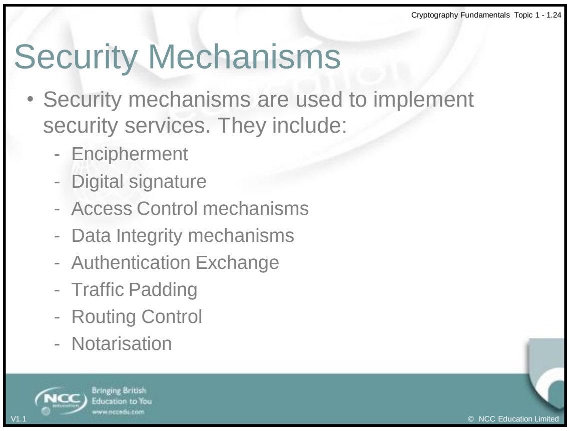
Cryptography Fundamentals Topic 1 - 1.23

Security Services

- A ***security service*** is a service which ensures adequate security of the systems or of data transfer.
- X.800 Recommendation divides security services into 5 categories:
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Non-repudiation

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



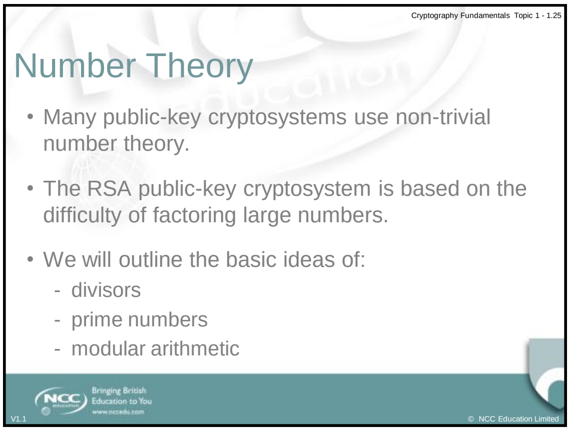
Cryptography Fundamentals Topic 1 - 1.24

Security Mechanisms

- Security mechanisms are used to implement security services. They include:
  - Encipherment
  - Digital signature
  - Access Control mechanisms
  - Data Integrity mechanisms
  - Authentication Exchange
  - Traffic Padding
  - Routing Control
  - Notarisation

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



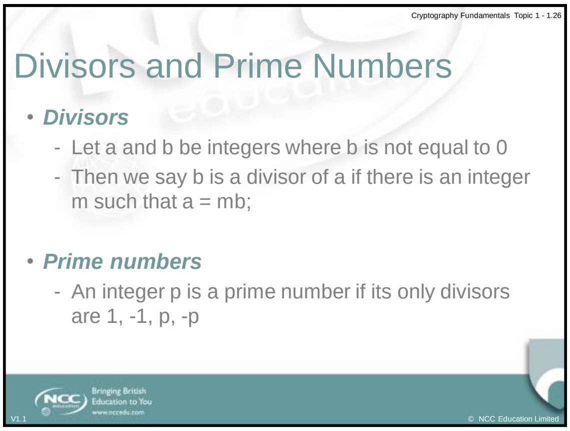
Cryptography Fundamentals Topic 1 - 1.25

Number Theory

- Many public-key cryptosystems use non-trivial number theory.
- The RSA public-key cryptosystem is based on the difficulty of factoring large numbers.
- We will outline the basic ideas of:
  - divisors
  - prime numbers
  - modular arithmetic

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



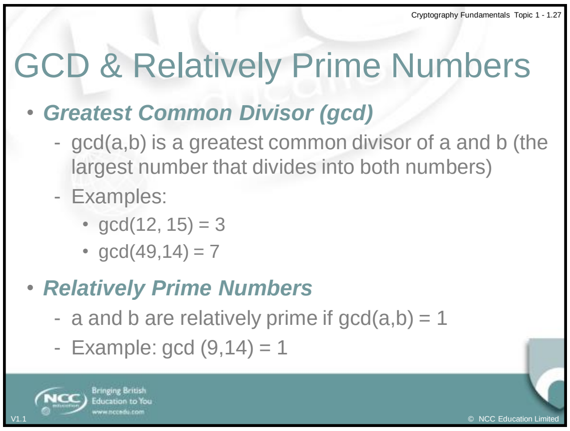
Cryptography Fundamentals Topic 1 - 1.26

Divisors and Prime Numbers

- ***Divisors***
  - Let a and b be integers where b is not equal to 0
  - Then we say b is a divisor of a if there is an integer m such that a = mb;
- ***Prime numbers***
  - An integer p is a prime number if its only divisors are 1, -1, p, -p

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



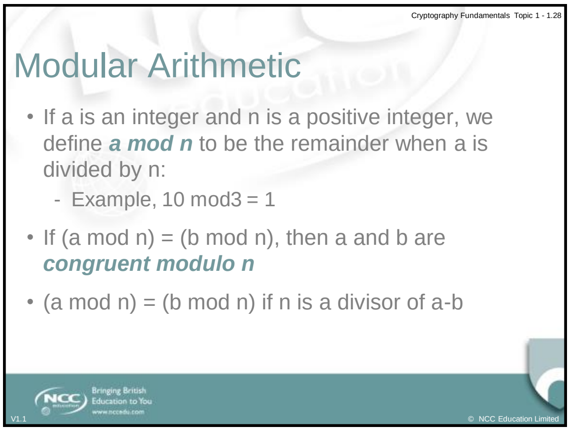
Cryptography Fundamentals Topic 1 - 1.27

GCD & Relatively Prime Numbers

- ***Greatest Common Divisor (gcd)***
  - gcd(a,b) is a greatest common divisor of a and b (the largest number that divides into both numbers)
  - Examples:
    - gcd(12, 15) = 3
    - gcd(49,14) = 7
- ***Relatively Prime Numbers***
  - a and b are relatively prime if gcd(a,b) = 1
  - Example: gcd (9,14) = 1

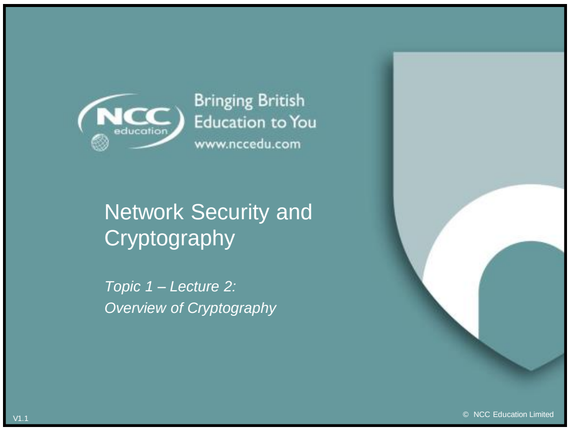
Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



Modular Arithmetic

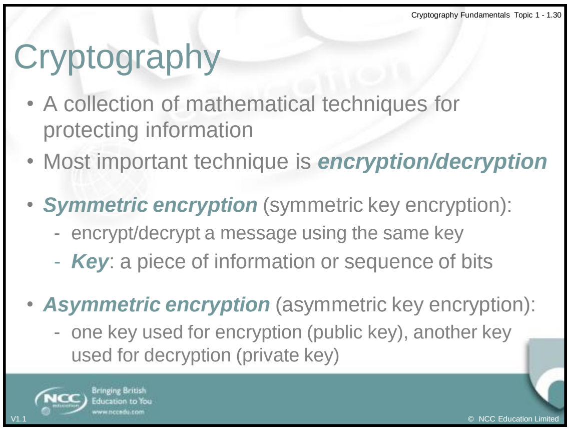
- If a is an integer and n is a positive integer, we define ***a mod n*** to be the remainder when a is divided by n:
  - Example, 10 mod3 = 1
- If (a mod n) = (b mod n), then a and b are ***congruent modulo n***
- (a mod n) = (b mod n) if n is a divisor of a-b



Bringing British Education to You
www.nccedu.com

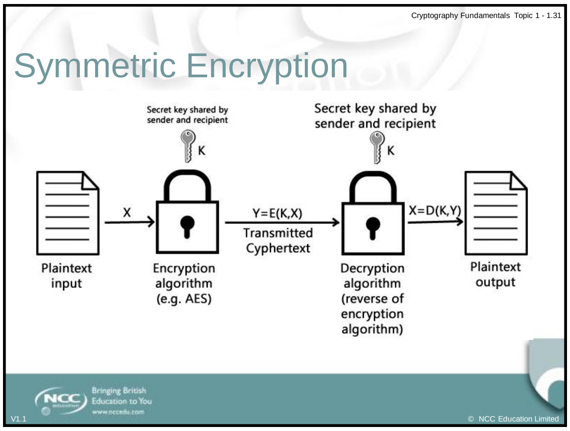
Network Security and Cryptography

Topic 1 – Lecture 2:
Overview of Cryptography



Cryptography

- A collection of mathematical techniques for protecting information
- Most important technique is ***encryption/decryption***
- ***Symmetric encryption*** (symmetric key encryption):
  - encrypt/decrypt a message using the same key
  - ***Key***: a piece of information or sequence of bits
- ***Asymmetric encryption*** (asymmetric key encryption):
  - one key used for encryption (public key), another key used for decryption (private key)



Cryptography Fundamentals Topic 1 - 1.31

Symmetric Encryption

Secret key shared by sender and recipient

K

Secret key shared by sender and recipient

K

X

Y=E(K,X)
Transmitted Cyphertext

X=D(K,Y)

Plaintext input

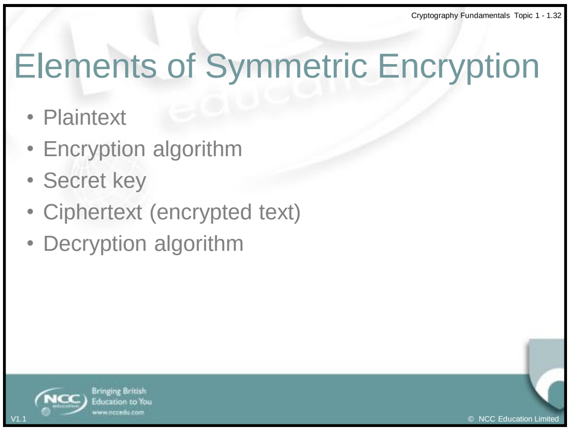
Encryption algorithm (e.g. AES)

Decryption algorithm (reverse of encryption algorithm)

Plaintext output

Bringing British Education to You www.nccedu.com

V1.1



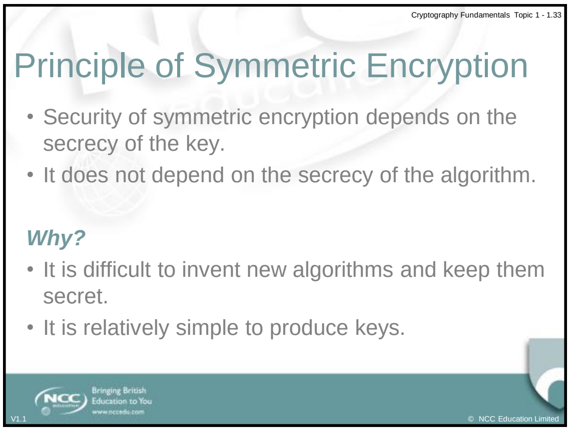
Cryptography Fundamentals Topic 1 - 1.32

Elements of Symmetric Encryption

- Plaintext
- Encryption algorithm
- Secret key
- Ciphertext (encrypted text)
- Decryption algorithm

Bringing British Education to You www.nccedu.com

V1.1



Cryptography Fundamentals Topic 1 - 1.33

Principle of Symmetric Encryption

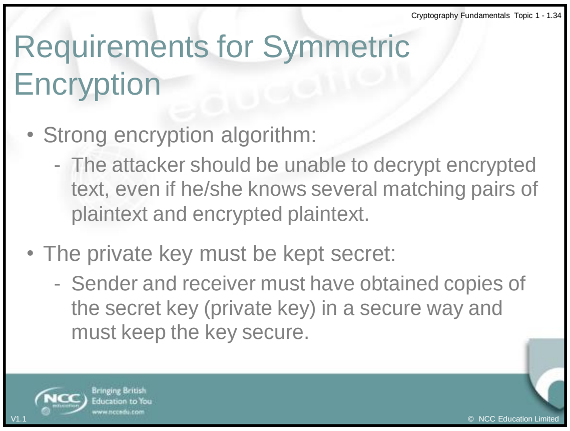
- Security of symmetric encryption depends on the secrecy of the key.
- It does not depend on the secrecy of the algorithm.

Why?

- It is difficult to invent new algorithms and keep them secret.
- It is relatively simple to produce keys.

Bringing British Education to You www.nccedu.com

V1.1

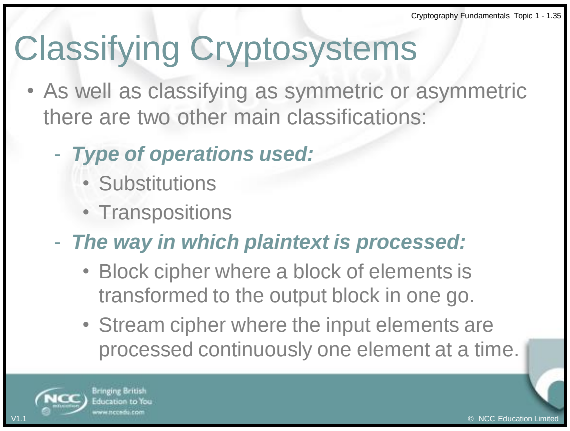


Cryptography Fundamentals Topic 1 - 1.34

Requirements for Symmetric Encryption

- Strong encryption algorithm:
  - The attacker should be unable to decrypt encrypted text, even if he/she knows several matching pairs of plaintext and encrypted plaintext.
- The private key must be kept secret:
  - Sender and receiver must have obtained copies of the secret key (private key) in a secure way and must keep the key secure.

V1.1

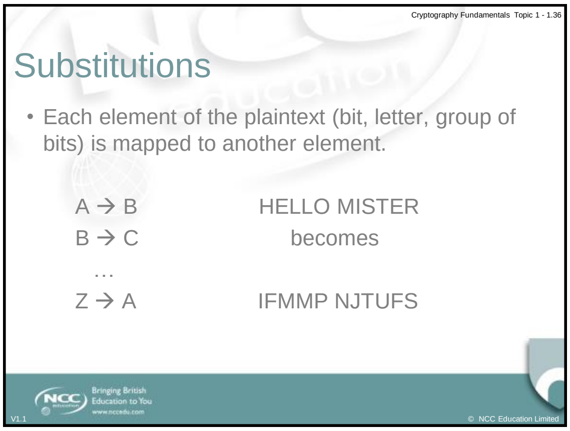


Cryptography Fundamentals Topic 1 - 1.35

Classifying Cryptosystems

- As well as classifying as symmetric or asymmetric there are two other main classifications:
  - ***Type of operations used:***
    - Substitutions
    - Transpositions
  - ***The way in which plaintext is processed:***
    - Block cipher where a block of elements is transformed to the output block in one go.
    - Stream cipher where the input elements are processed continuously one element at a time.

V1.1



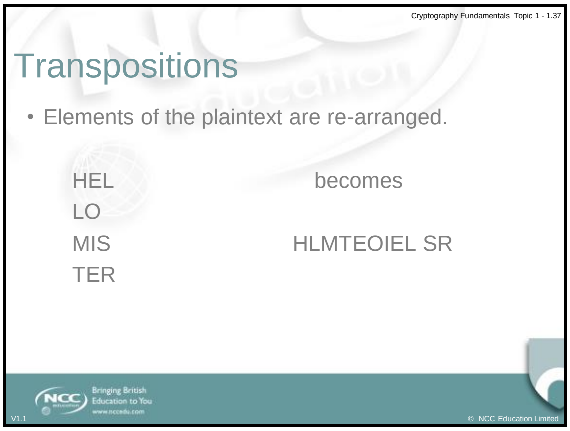
Cryptography Fundamentals Topic 1 - 1.36

Substitutions

- Each element of the plaintext (bit, letter, group of bits) is mapped to another element.

A → B	HELLO MISTER
B → C	becomes
…	
Z → A	IFMMP NJTUFS

V1.1



Cryptography Fundamentals Topic 1 - 1.37

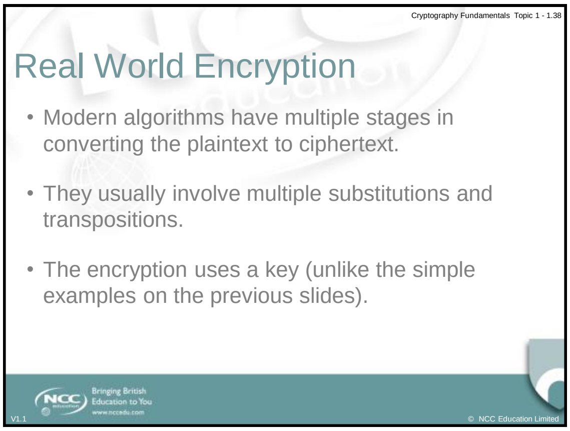
Transpositions

- Elements of the plaintext are re-arranged.

HEL LO MIS TER	becomes HLMTEOIEL SR

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



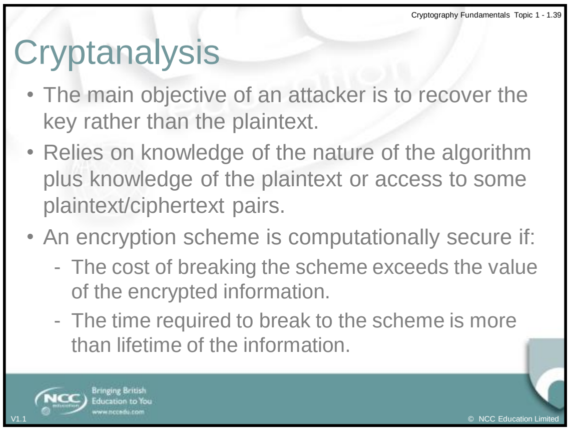
Cryptography Fundamentals Topic 1 - 1.38

Real World Encryption

- Modern algorithms have multiple stages in converting the plaintext to ciphertext.
- They usually involve multiple substitutions and transpositions.
- The encryption uses a key (unlike the simple examples on the previous slides).

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



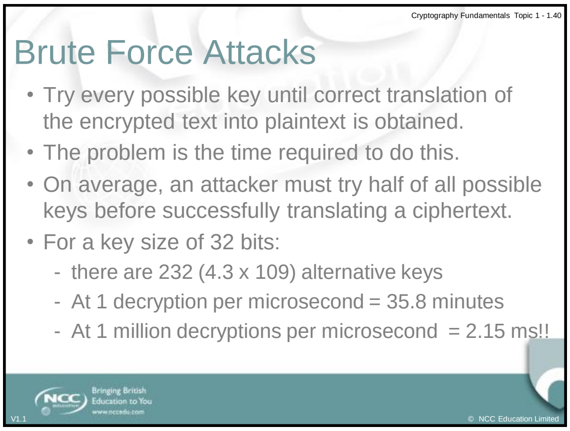
Cryptography Fundamentals Topic 1 - 1.39

Cryptanalysis

- The main objective of an attacker is to recover the key rather than the plaintext.
- Relies on knowledge of the nature of the algorithm plus knowledge of the plaintext or access to some plaintext/ciphertext pairs.
- An encryption scheme is computationally secure if:
  - The cost of breaking the scheme exceeds the value of the encrypted information.
  - The time required to break to the scheme is more than lifetime of the information.

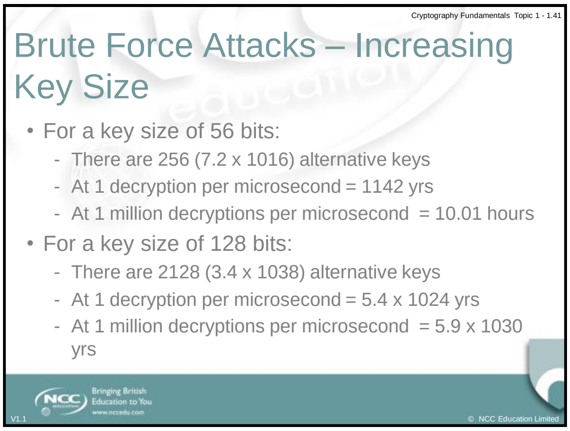
Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



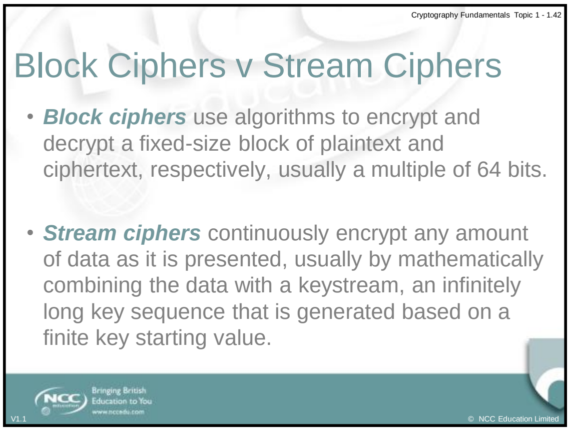
Brute Force Attacks

- Try every possible key until correct translation of the encrypted text into plaintext is obtained.
- The problem is the time required to do this.
- On average, an attacker must try half of all possible keys before successfully translating a ciphertext.
- For a key size of 32 bits:
  - there are 232 (4.3 x 109) alternative keys
  - At 1 decryption per microsecond = 35.8 minutes
  - At 1 million decryptions per microsecond = 2.15 ms!!



Brute Force Attacks – Increasing Key Size

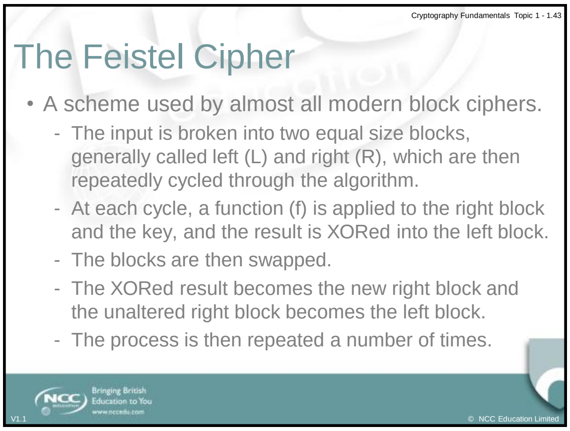
- For a key size of 56 bits:
  - There are 256 (7.2 x 1016) alternative keys
  - At 1 decryption per microsecond = 1142 yrs
  - At 1 million decryptions per microsecond = 10.01 hours
- For a key size of 128 bits:
  - There are 2128 (3.4 x 1038) alternative keys
  - At 1 decryption per microsecond = 5.4 x 1024 yrs
  - At 1 million decryptions per microsecond = 5.9 x 1030 yrs



Block Ciphers v Stream Ciphers

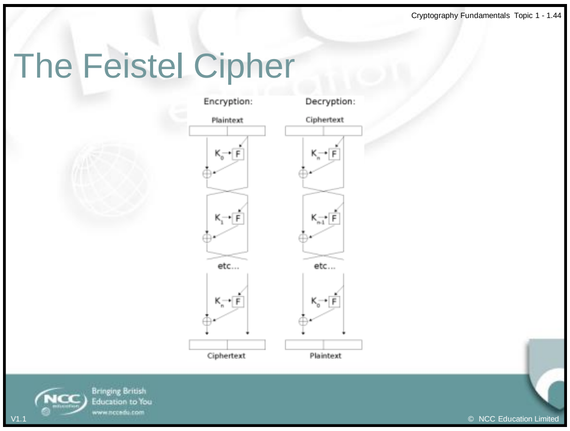
- ***Block ciphers*** use algorithms to encrypt and decrypt a fixed-size block of plaintext and ciphertext, respectively, usually a multiple of 64 bits.

- ***Stream ciphers*** continuously encrypt any amount of data as it is presented, usually by mathematically combining the data with a keystream, an infinitely long key sequence that is generated based on a finite key starting value.

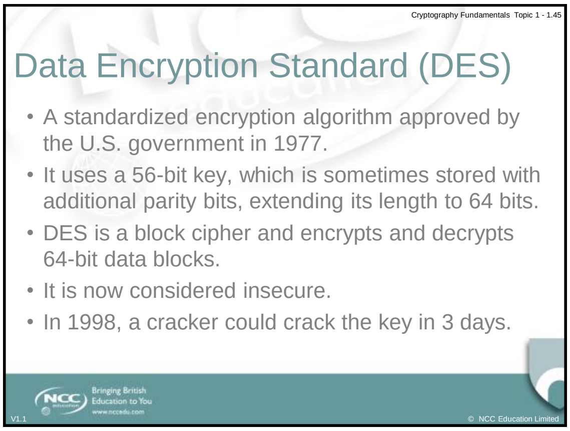


The Feistel Cipher

- A scheme used by almost all modern block ciphers.
  - The input is broken into two equal size blocks, generally called left (L) and right (R), which are then repeatedly cycled through the algorithm.
  - At each cycle, a function (f) is applied to the right block and the key, and the result is XORed into the left block.
  - The blocks are then swapped.
  - The XORed result becomes the new right block and the unaltered right block becomes the left block.
  - The process is then repeated a number of times.

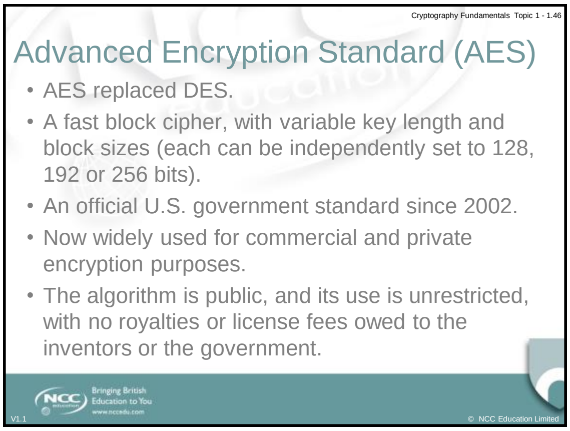


The Feistel Cipher



Data Encryption Standard (DES)

- A standardized encryption algorithm approved by the U.S. government in 1977.
- It uses a 56-bit key, which is sometimes stored with additional parity bits, extending its length to 64 bits.
- DES is a block cipher and encrypts and decrypts 64-bit data blocks.
- It is now considered insecure.
- In 1998, a cracker could crack the key in 3 days.



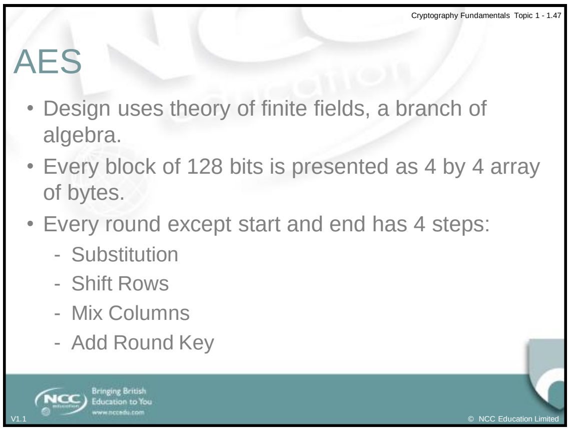
Cryptography Fundamentals Topic 1 - 1.46

Advanced Encryption Standard (AES)

- AES replaced DES.
- A fast block cipher, with variable key length and block sizes (each can be independently set to 128, 192 or 256 bits).
- An official U.S. government standard since 2002.
- Now widely used for commercial and private encryption purposes.
- The algorithm is public, and its use is unrestricted, with no royalties or license fees owed to the inventors or the government.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



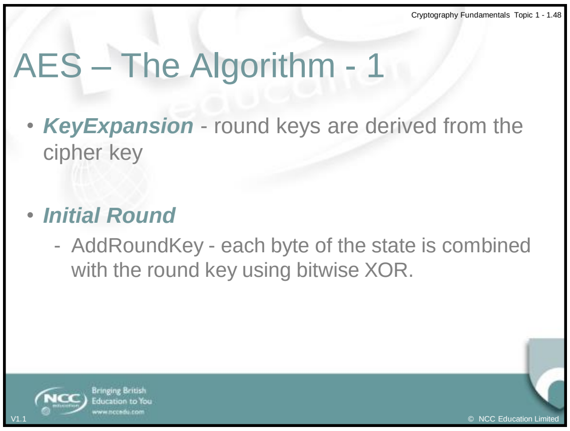
Cryptography Fundamentals Topic 1 - 1.47

AES

- Design uses theory of finite fields, a branch of algebra.
- Every block of 128 bits is presented as 4 by 4 array of bytes.
- Every round except start and end has 4 steps:
  - Substitution
  - Shift Rows
  - Mix Columns
  - Add Round Key

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



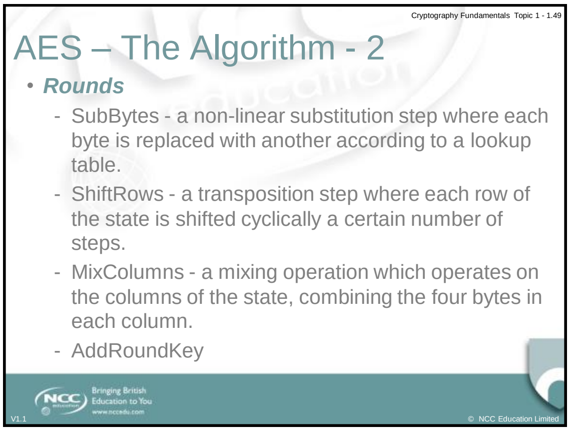
Cryptography Fundamentals Topic 1 - 1.48

AES – The Algorithm - 1

- ***KeyExpansion*** - round keys are derived from the cipher key
- ***Initial Round***
  - AddRoundKey - each byte of the state is combined with the round key using bitwise XOR.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



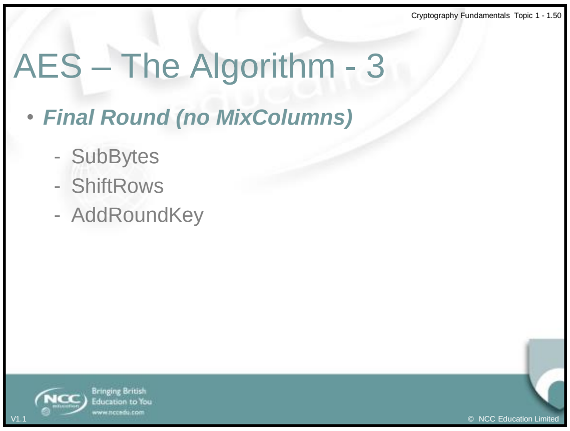
Cryptography Fundamentals Topic 1 - 1.49

AES – The Algorithm - 2

- ***Rounds***
  - SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
  - ShiftRows - a transposition step where each row of the state is shifted cyclically a certain number of steps.
  - MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
  - AddRoundKey

Bringing British Education to You www.nccedu.com

V1.1



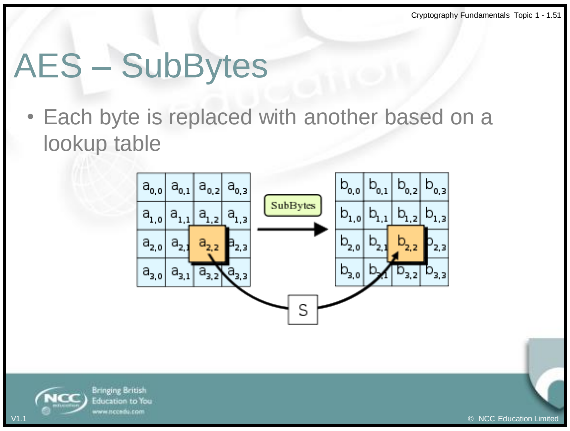
Cryptography Fundamentals Topic 1 - 1.50

AES – The Algorithm - 3

- ***Final Round (no MixColumns)***
  - SubBytes
  - ShiftRows
  - AddRoundKey

Bringing British Education to You www.nccedu.com

V1.1



Cryptography Fundamentals Topic 1 - 1.51

AES – SubBytes

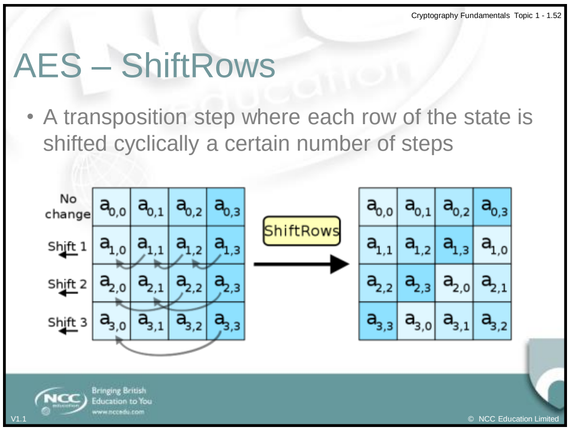
- Each byte is replaced with another based on a lookup table

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

Bringing British Education to You www.nccedu.com

V1.1



AES – ShiftRows

- A transposition step where each row of the state is shifted cyclically a certain number of steps

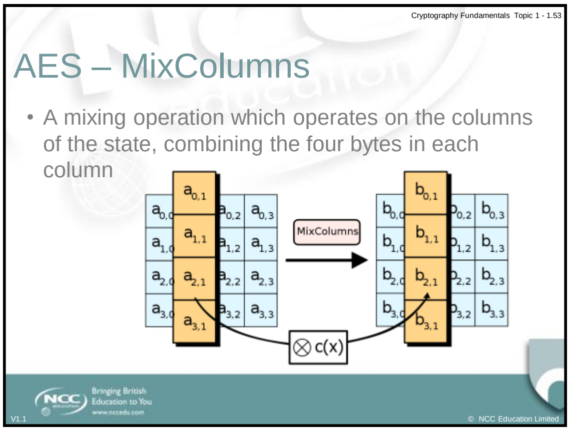
No change	$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
Shift 1	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
Shift 2	$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
Shift 3	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

ShiftRows

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,0}$
$a_{2,2}$	$a_{2,3}$	$a_{2,0}$	$a_{2,1}$
$a_{3,3}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



AES – MixColumns

- A mixing operation which operates on the columns of the state, combining the four bytes in each column

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

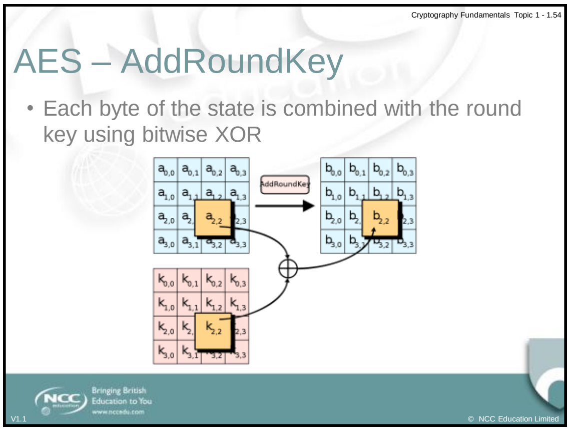
MixColumns

$\otimes c(x)$

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



AES – AddRoundKey

- Each byte of the state is combined with the round key using bitwise XOR

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

AddRoundKey

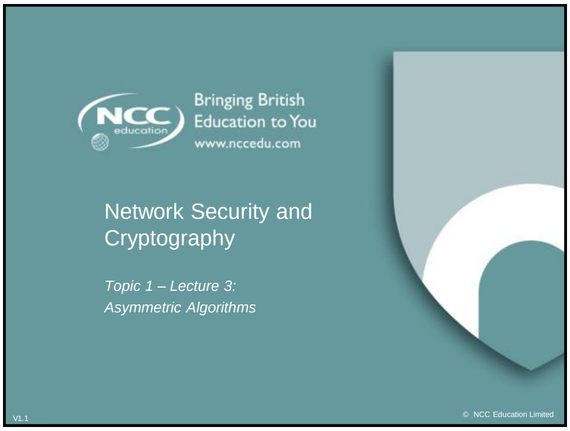
$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

$\oplus$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited

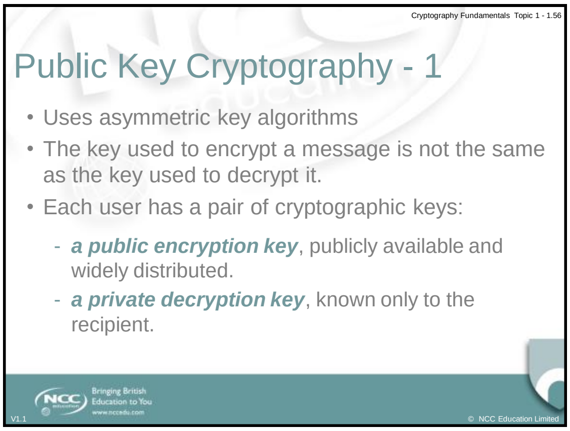


Bringing British Education to You
www.nccedu.com

Network Security and Cryptography

Topic 1 – Lecture 3:
Asymmetric Algorithms

V1.1



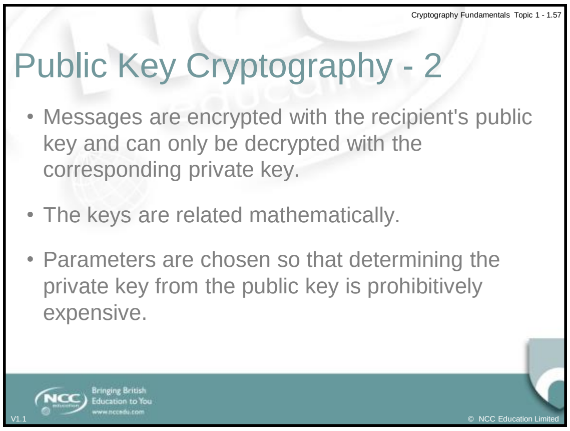
Cryptography Fundamentals Topic 1 - 1.56

Public Key Cryptography - 1

- Uses asymmetric key algorithms
- The key used to encrypt a message is not the same as the key used to decrypt it.
- Each user has a pair of cryptographic keys:
  - ***a public encryption key***, publicly available and widely distributed.
  - ***a private decryption key***, known only to the recipient.

Bringing British Education to You
www.nccedu.com

V1.1



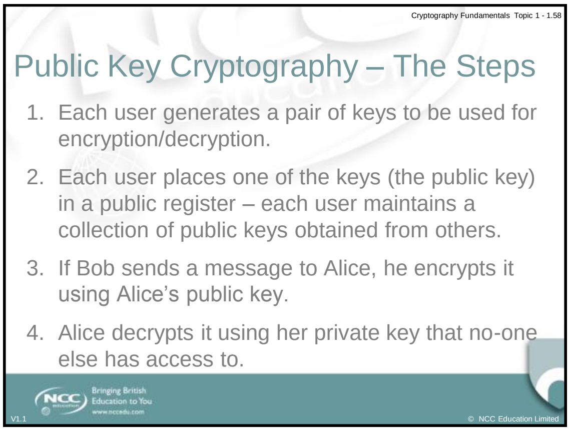
Cryptography Fundamentals Topic 1 - 1.57

Public Key Cryptography - 2

- Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key.
- The keys are related mathematically.
- Parameters are chosen so that determining the private key from the public key is prohibitively expensive.

Bringing British Education to You
www.nccedu.com

V1.1



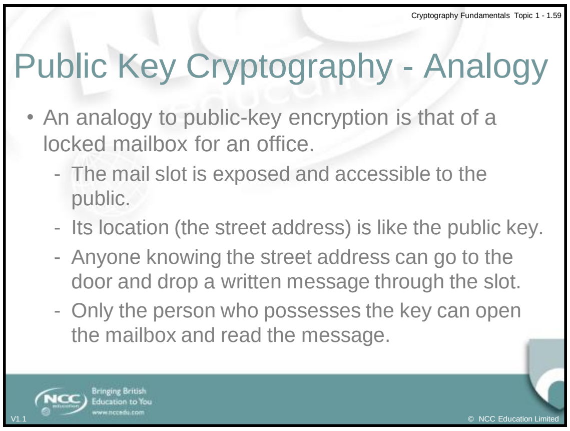
Cryptography Fundamentals Topic 1 - 1.58

Public Key Cryptography – The Steps

1. Each user generates a pair of keys to be used for encryption/decryption.
2. Each user places one of the keys (the public key) in a public register – each user maintains a collection of public keys obtained from others.
3. If Bob sends a message to Alice, he encrypts it using Alice's public key.
4. Alice decrypts it using her private key that no-one else has access to.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



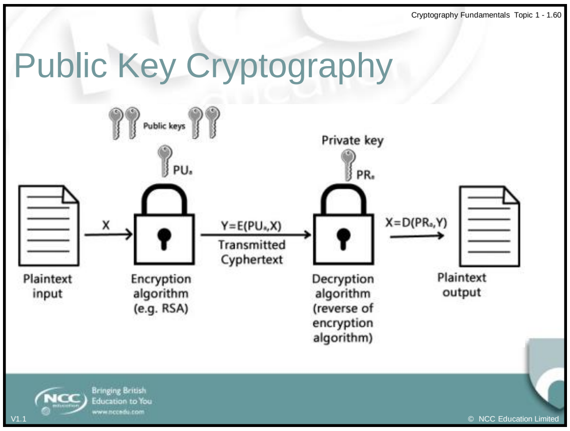
Cryptography Fundamentals Topic 1 - 1.59

Public Key Cryptography - Analogy

- An analogy to public-key encryption is that of a locked mailbox for an office.
  - The mail slot is exposed and accessible to the public.
  - Its location (the street address) is like the public key.
  - Anyone knowing the street address can go to the door and drop a written message through the slot.
  - Only the person who possesses the key can open the mailbox and read the message.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



Cryptography Fundamentals Topic 1 - 1.60

Public Key Cryptography

Public keys

PU_a

Private key

PR_a

X

$Y=E(PU_a,X)$

Transmitted Cyphertext

$X=D(PR_a,Y)$

Plaintext input

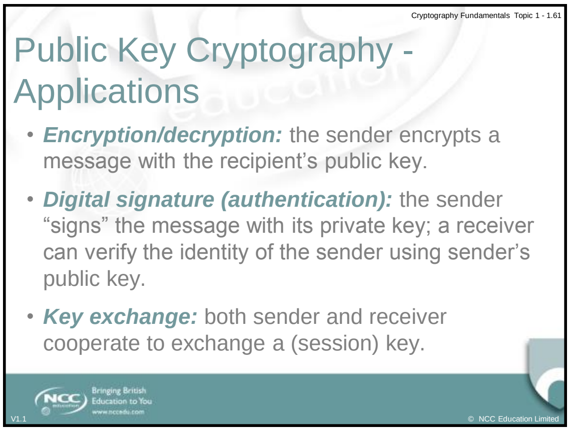
Encryption algorithm (e.g. RSA)

Decryption algorithm (reverse of encryption algorithm)

Plaintext output

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited

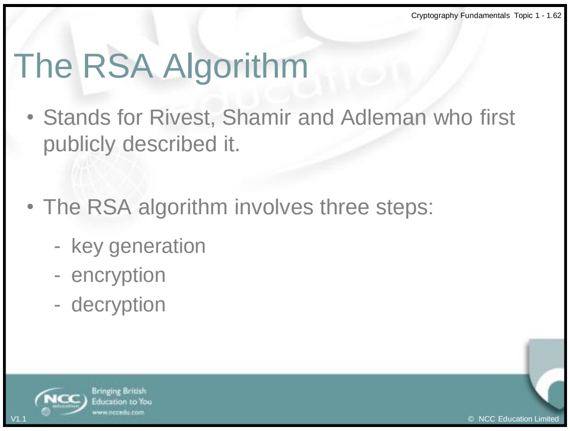


Cryptography Fundamentals Topic 1 - 1.61

Public Key Cryptography - Applications

- ***Encryption/decryption:*** the sender encrypts a message with the recipient's public key.
- ***Digital signature (authentication):*** the sender "signs" the message with its private key; a receiver can verify the identity of the sender using sender's public key.
- ***Key exchange:*** both sender and receiver cooperate to exchange a (session) key.

V1.1 © NCC Education Limited

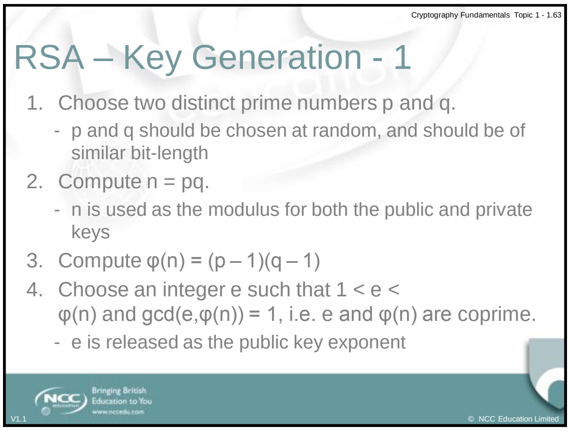


Cryptography Fundamentals Topic 1 - 1.62

The RSA Algorithm

- Stands for Rivest, Shamir and Adleman who first publicly described it.
- The RSA algorithm involves three steps:
  - key generation
  - encryption
  - decryption

V1.1 © NCC Education Limited

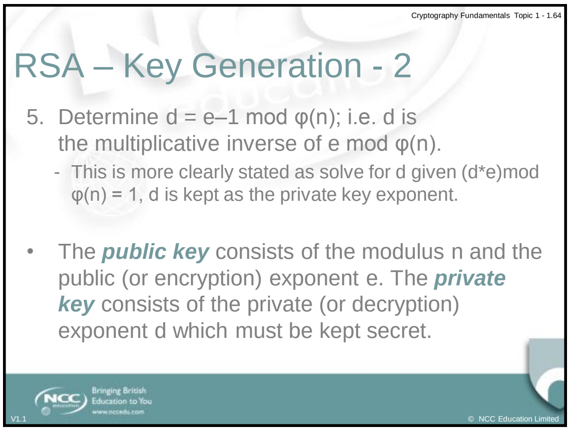


Cryptography Fundamentals Topic 1 - 1.63

RSA – Key Generation - 1

1. Choose two distinct prime numbers p and q.
   - p and q should be chosen at random, and should be of similar bit-length
2. Compute n = pq.
   - n is used as the modulus for both the public and private keys
3. Compute $\varphi(n) = (p – 1)(q – 1)$
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e,\varphi(n)) = 1$, i.e. e and $\varphi(n)$ are coprime.
   - e is released as the public key exponent

V1.1 © NCC Education Limited



Cryptography Fundamentals Topic 1 - 1.64

RSA – Key Generation - 2

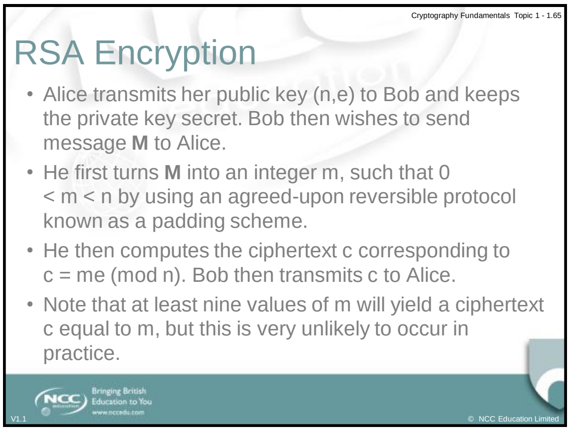
5. Determine d = e–1 mod φ(n); i.e. d is the multiplicative inverse of e mod φ(n).
   - This is more clearly stated as solve for d given (d*e)mod φ(n) = 1, d is kept as the private key exponent.

- The ***public key*** consists of the modulus n and the public (or encryption) exponent e. The ***private key*** consists of the private (or decryption) exponent d which must be kept secret.

Bringing British Education to You www.nccedu.com

V1.1

© NCC Education Limited



Cryptography Fundamentals Topic 1 - 1.65

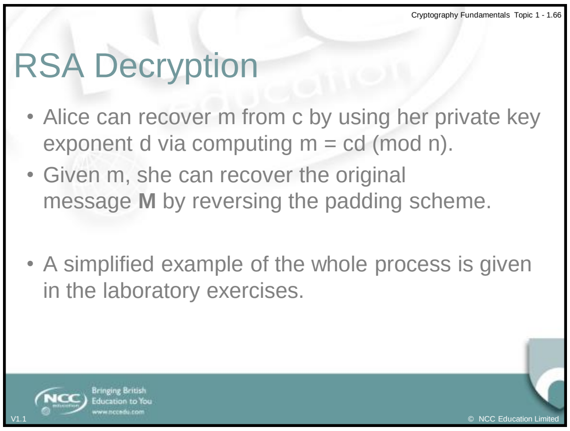
RSA Encryption

- Alice transmits her public key (n,e) to Bob and keeps the private key secret. Bob then wishes to send message **M** to Alice.
- He first turns **M** into an integer m, such that 0 < m < n by using an agreed-upon reversible protocol known as a padding scheme.
- He then computes the ciphertext c corresponding to c = me (mod n). Bob then transmits c to Alice.
- Note that at least nine values of m will yield a ciphertext c equal to m, but this is very unlikely to occur in practice.

Bringing British Education to You www.nccedu.com

V1.1

© NCC Education Limited



Cryptography Fundamentals Topic 1 - 1.66

RSA Decryption

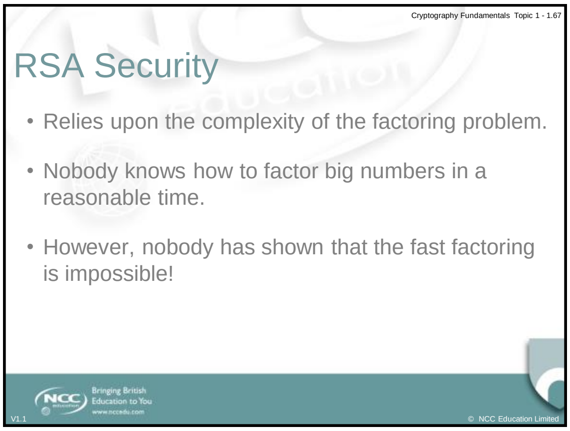
- Alice can recover m from c by using her private key exponent d via computing m = cd (mod n).
- Given m, she can recover the original message **M** by reversing the padding scheme.

- A simplified example of the whole process is given in the laboratory exercises.

Bringing British Education to You www.nccedu.com

V1.1

© NCC Education Limited



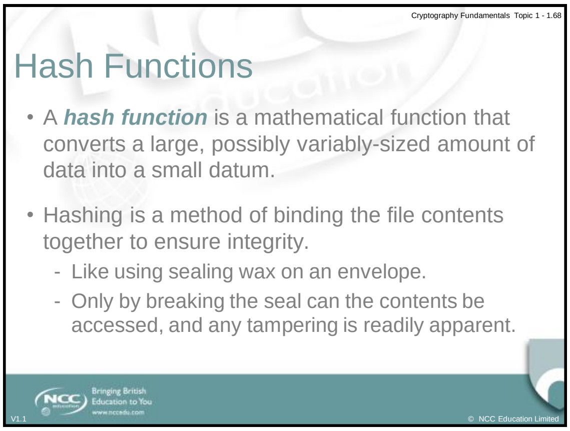
Cryptography Fundamentals Topic 1 - 1.67

RSA Security

- Relies upon the complexity of the factoring problem.
- Nobody knows how to factor big numbers in a reasonable time.
- However, nobody has shown that the fast factoring is impossible!

V1.1

© NCC Education Limited



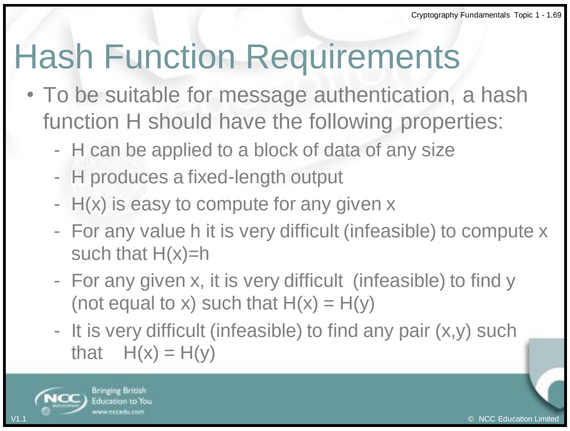
Cryptography Fundamentals Topic 1 - 1.68

Hash Functions

- A ***hash function*** is a mathematical function that converts a large, possibly variably-sized amount of data into a small datum.
- Hashing is a method of binding the file contents together to ensure integrity.
  - Like using sealing wax on an envelope.
  - Only by breaking the seal can the contents be accessed, and any tampering is readily apparent.

V1.1

© NCC Education Limited



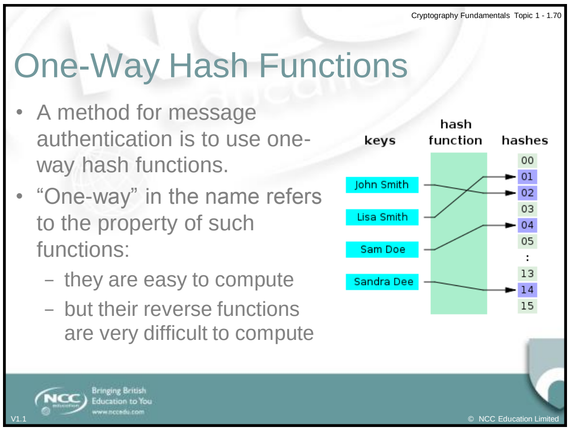
Cryptography Fundamentals Topic 1 - 1.69

Hash Function Requirements

- To be suitable for message authentication, a hash function H should have the following properties:
  - H can be applied to a block of data of any size
  - H produces a fixed-length output
  - H(x) is easy to compute for any given x
  - For any value h it is very difficult (infeasible) to compute x such that H(x)=h
  - For any given x, it is very difficult (infeasible) to find y (not equal to x) such that H(x) = H(y)
  - It is very difficult (infeasible) to find any pair (x,y) such that H(x) = H(y)

V1.1

© NCC Education Limited



Cryptography Fundamentals Topic 1 - 1.70

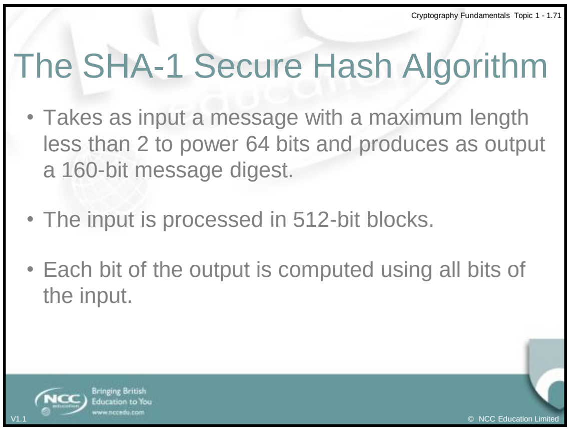
One-Way Hash Functions

- A method for message authentication is to use one-way hash functions.
- “One-way” in the name refers to the property of such functions:
  - they are easy to compute
  - but their reverse functions are very difficult to compute

keys
hash function
hashes
John Smith
Lisa Smith
Sam Doe
Sandra Dee
00
01
02
03
04
05
:
13
14
15

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



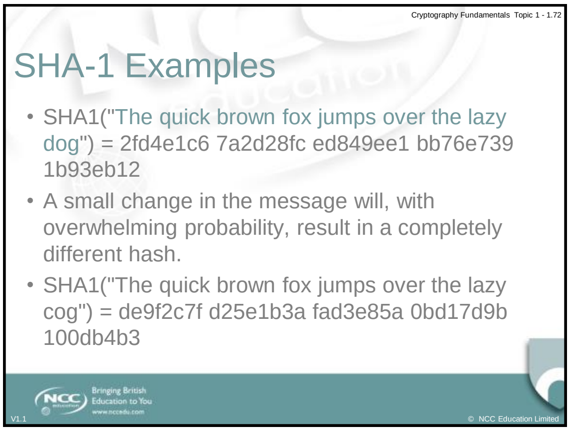
Cryptography Fundamentals Topic 1 - 1.71

The SHA-1 Secure Hash Algorithm

- Takes as input a message with a maximum length less than 2 to power 64 bits and produces as output a 160-bit message digest.
- The input is processed in 512-bit blocks.
- Each bit of the output is computed using all bits of the input.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



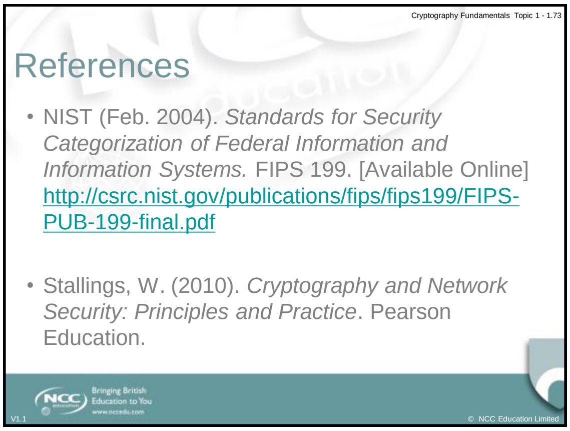
Cryptography Fundamentals Topic 1 - 1.72

SHA-1 Examples

- SHA1("The quick brown fox jumps over the lazy dog") = 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
- A small change in the message will, with overwhelming probability, result in a completely different hash.
- SHA1("The quick brown fox jumps over the lazy cog") = de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



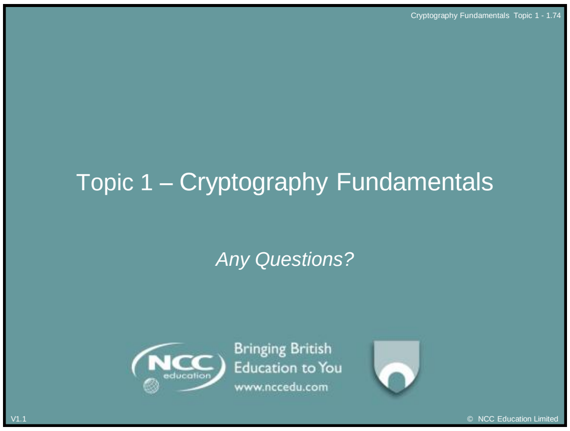
Cryptography Fundamentals Topic 1 - 1.73

References

- NIST (Feb. 2004). *Standards for Security Categorization of Federal Information and Information Systems.* FIPS 199. [Available Online] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Stallings, W. (2010). *Cryptography and Network Security: Principles and Practice*. Pearson Education.

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited



Cryptography Fundamentals Topic 1 - 1.74

Topic 1 – Cryptography Fundamentals

Any Questions?

Bringing British Education to You www.nccedu.com

V1.1 © NCC Education Limited