UNIVERSITY OF WESTMINSTER

Cryptography

6COSC019W- Cyber Security

Dr Ayman El Hajjar

February 06, 2023

School of Computer Science and Engineering
University of Westminster

OUTLINE

Cryptography- The Math

Why the Math?

- Cryptography is no different from most computer science disciplines in that it finds its foundations in the science of mathematics.
- To fully understand cryptography, you must first understand the basics of binary mathematics, and the logical operations used to manipulate binary values.
- We also need to understand some arithmetic concepts and prime numbers.

BOOLEAN MATHEMATICS MATHEMATICS

- Boolean mathematics defines the rules used for the bits and bytes that form the nervous system of any computer. You're most likely familiar with the decimal system.
- It is a base 10 system in which an integer from 0 to 9 is used in each place and each place value is a multiple of 10.
- It's likely that our reliance on the decimal system has biological origins—human beings have 10 fingers that can be used to count.
- The Boolean mathematics of cryptography uses a variety of logical functions to manipulate data.

AND OPERATION

- The AND operation (represented by the $\wedge$ symbol) checks to see whether two values are both true.
- The truth table that follows illustrates all four possible outputs for the AND function.

X	Y	X ∧ Y
0	0	0
0	1	0
1	0	0
1	1	1

```
X:     0 1 1 0 1 1 0 0
Y:     1 0 1 0 0 1 1 1
-----------------------
X ∧ Y: 0 0 1 0 0 1 0 0
```

OR OPERATION

- The OR operation (represented by the $\vee$ symbol) checks to see whether at least one of the input values is true.
- The following truth table for all possible values of the OR function

X	Y	X ∨ Y
0	0	0
0	1	1
1	0	1
1	1	1

```
X:     0 1 1 0 1 1 0 0
Y:     1 0 1 0 0 1 1 1
_____________________
X V Y:   1 1 1 0 1 1 1 1
```

NOT OPERATION

- The NOT operation (represented by the $\sim$ or ! symbol) simply reverses the value of an input variable.
- This function operates on only one variable at a time.
- Here's the truth table for the NOT function:

X	~X
0	1
1	0

```
 X:      0 1 1 0 1 1 0 0
-------------------------
~X:      1 0 0 1 0 0 1 1
```

XOR OPERATION

- The final logical function we'll examine is perhaps the most important and most commonly used in cryptographic applications—the exclusive OR (XOR) function.
- It's referred to in mathematical literature as the XOR function and is commonly represented by the $\oplus$ symbol.
- The XOR function returns a true value when only one of the input values is true.
- If both values are false or both values are true, the output of the XOR function is false. Here is the truth table for the XOR operation:

XOR OPERATION

X	Y	X ⊕ Y
0	0	0
0	1	1
1	0	1
1	1	0

```
     X:   0 1 1 0 1 1 0 0
     Y:   1 0 1 0 0 1 1 1
-------------------------
X ⊕ Y:   1 1 0 0 1 0 1 1
```

PRIME NUMBER

- Prime numbers only have divisors of 1 and itself
  - ☞ They cannot be written as a product of other numbers
- Prime numbers are central to number theory

First few prime numbers

The first few prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29.

Euclidean Algorithm

- One of the basic techniques of number theory
- Procedure for determining the greatest common divisor of two positive integers
- Two integers are relatively prime if their only common positive integer factor is 1

Greatest Common Divisor (GCD)

8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

FERMAT'S THEOREM

- States the following:
  - If p is prime and a is a positive integer not divisible by p then
    - $a^{p-1} \quad 1(mod(p))$

Modulus Function

Modulus

If a is an integer and n is a positive integer, we define $amodn$ to be the remainder when a is divided by n; the integer n is called the modulus

- The modulo function is extremely important in the field of cryptography.
- Computers don't naturally understand the decimal system, and these remainder values play a critical role when computers perform many mathematical functions.
- The **Modulus function** is, quite simply, the remainder value left over after a division operation is performed.

Modulus Function

- The modulo function is usually represented in equations by the abbreviation mod although it's also sometimes represented by the % operator.
- Thus, for any integer a:

$a \quad qn + r0 \leq r \leq n; q \quad [\frac{a}{n}]$

☞ $a \quad [\frac{a}{n}] * n + (a\%n)$

Modulus Examples

☞ 11 mod(7) 4 , or 11%7 4

☞ 11 mod(7) 3 , or 11%7 3

Nonce

- Cryptography often gains strength by adding randomness to the encryption process.
- One method by which this is accomplished is through the use of a nonce.
- A nonce is a random number generator. It acts as a placeholder variable in mathematical functions.
- When the function is executed, the nonce is replaced with a random number generated at the moment of processing.
- The nonce produces a unique number each time it is used.

Nonces: Initialization Vectors

- Initialization vectors (IVs) are random values that are used with algorithms to ensure patterns are not created during the encryption process.
- They are used with keys and do not need to be encrypted when being sent to the destination.
- If IVs are not used, then two identical plaintext values that are encrypted with the same key will create the same ciphertext.
- Providing attackers with these types of patterns can make their job easier in breaking the encryption method and uncovering the key.

Cryptography- An overview

CRYPTOGRAPHY TERMS

- **Cryptography** The area of study of the many schemes used for encryption
- **Cryptanalysis** Techniques used for deciphering a message without any knowledge of the enciphering details
- **Unencrypted information**—Information in understandable form (plaintext or cleartext)
- **Encrypted information**—Information in scrambled form (ciphertext)
- **Encryption**—The process of scrambling plaintext into ciphertext (or Enciphering)
- **Decryption**—The process of unscrambling ciphertext into plaintext (or Deciphering)
- **Cryptographic algorithm/cipher** A scheme

CRYPTOGRAPHY CONCEPT

Cryptography

- Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process.
- It is considered a science of protecting information by encoding it into an unreadable format.
- Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through untrusted network communication paths.

Cryptography Goals

Cryptography Goals

- The most important goal is to hide information from unauthorized individuals.
- With enough time, resources, and motivation, hackers can break most algorithms and reveal the encoded information.
- A more realistic goal of cryptography is to make obtaining the information too work-intensive or time-consuming to be worthwhile to the attacker.

Cryptosystems Basics

Goals of cryptography

Security practitioners use cryptographic systems to meet four fundamental goals:

- confidentiality, integrity, authentication, and non-repudiation.

Achieving each of these goals requires the satisfaction of a number of design requirements, and not all cryptosystems are intended to achieve all four goals.

CONFIDENTIALITY IN CRYPTOSYSTEMS

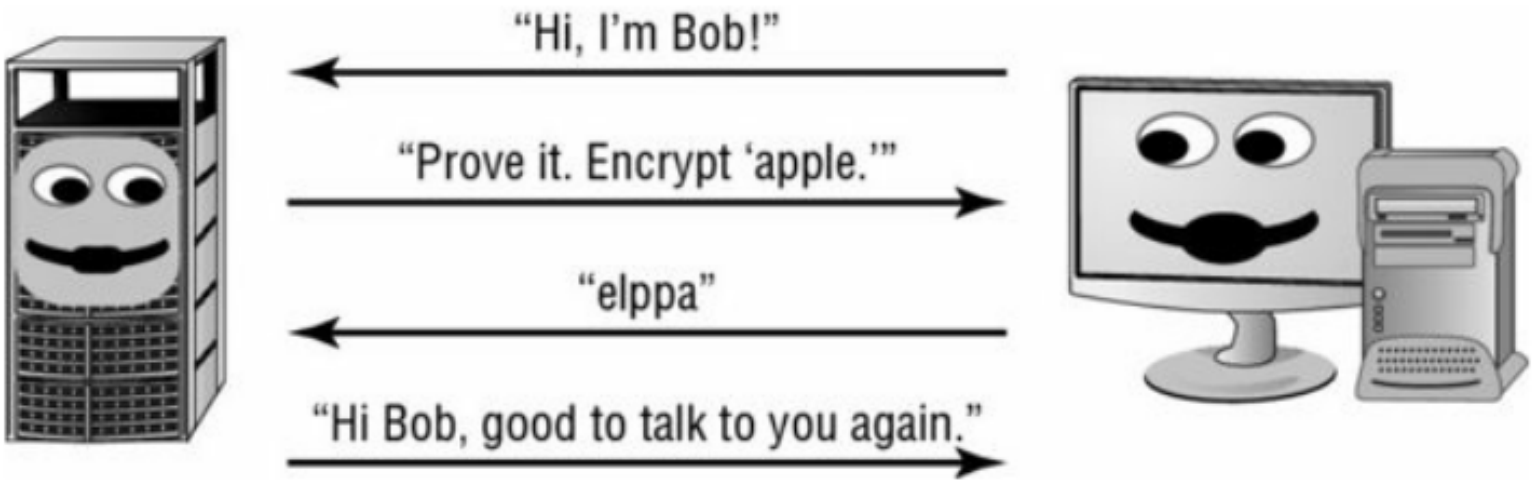
- Two main types of cryptosystems enforce confidentiality.
  - Symmetric key cryptosystems use a shared secret key available to all users of the cryptosystem.
  - Asymmetric cryptosystems use individual combinations of public and private keys for each user of the system.
- When developing a cryptographic system for the purpose of providing confidentiality, we must think about two different types of data:
  - **Data at rest**, or stored data, is that which resides in a permanent location awaiting access.
  - **Data in motion,** or data "on the wire, is data being transmitted across a network between two systems.

INTEGRITY IN CRYPTOSYSTEMS

- **Integrity** ensures that data is not altered without authorization.
- It allows to:
  - Check if message received is identical to the sent message.
  - Ensure that stored data was not altered between the time it was created and the time it was accessed.
  - Protect against all forms of alteration.
- **Message integrity** is enforced through the use of encrypted message digests, known as **digital signatures** created upon transmission of a message
- Integrity can be enforced by both public and secret key cryptosystems.

AUTHENTICATION IN CRYPTOSYSTEMS

- **Authentication** verifies the claimed identity of system users and is a major function of cryptosystems



Challenge-response authentication protocol

NON-REPUDIATION IN CRYPTOSYSTEMS

- **Nonrepudiation** provides assurance to the recipient that the message was originated by the sender and not someone masquerading as the sender.
- It also prevents the sender from claiming that they never sent the message in the first place (also known as repudiating the message).

CRYPTOSYSTEMS

Cryptosystems

A **cryptosystem** encompasses all of the necessary components for encryption and decryption to take place. Pretty Good Privacy (PGP) is just one example of a cryptosystem. A **cryptosystem** is made up of at least the following:

- Software
- Protocols
- Algorithms
- Keys

Cryptography Capabilities

- Privacy or confidentiality
- Integrity
- Entity authentication or identification
- Message authentication
- Signature
- Access control
- Certification
- Timestamping
- Witnessing
- Ownership
- Anonymity
- Non-repudiation

Cryptographic Functions and Ciphers

- Each cipher has specific characteristics that make it desirable or undesirable
- When evaluating a cipher, consider its intended use
  - Are you trying to secure data in transit or data at rest?
  - Different ciphers solve different problems better than others
- After selecting a cipher, you must make additional decisions about key size, operational mode, etc.
- Many symmetric ciphers operate as either a stream cipher or a block cipher

Confusion and Diffusion

- Cryptographic algorithms rely upon two basic operations to obscure plain-text messages—confusion and diffusion.
- Confusion occurs when the relationship between the plain text and the key is so complicated that an attacker can't merely continue altering the plain text and analyzing the resulting cipher text to determine the key.
- Diffusion occurs when a change in the plain text results in multiple changes spread throughout the cipher text.

STEGANOGRAPHY

- Steganography is a method of hiding data in another media type so the very existence of the data is concealed.
- Only the sender and receiver are supposed to be able to see the message because it is secretly hidden in a graphic, wave file, document, or other type of media.
  - The message is not encrypted, just hidden.
  - Encrypted messages can draw attention because it tells the bad guy, “This is something sensitive.
  - A message hidden in a picture of your dog would not attract this type of attention, even though the same secret message can be embedded into this image.
    - Steganography is a type of security through obscurity.
    - Media files are ideal for steganographic transmission because of their large size.

THE STRENGTH OF THE CRYPTOSYSTEM

- The **strength of an encryption** method comes from
  - The algorithm
  - The secrecy of the key
  - The length of the key
  - The initialization vectors
  - How they all work together within the cryptosystem.
- The strength of an encryption method correlates to:
  - The amount of necessary processing power
  - Resources
  - and time required to break the cryptosystem or to figure out the value of the key.

THE STRENGTH OF THE CRYPTOSYSTEM

- Breaking a cryptosystem can be accomplished by a brute force attack
  - If a key can be broken with a Pentium Core i7 processor in three hours, the cipher is not strong at all.
  - If the key can only be broken with the use of a thousand multiprocessing systems over 1.2 million years, then it is pretty darn strong.
    - The introduction of mutli-core processors has really increased the threat of brute force attacks.

Cryptographic Systems

CRYPTOGRAPHIC SYSTEMS

✺ A cryptographic System is characterized along three independent dimensions:

✘ The type of operations used for transforming plaintext to ciphertext

- ☞ Substitution
- ☞ Transposition

✘ The number of keys used

- ☞ Symmetric
- ☞ Asymmetric

✘ The way in which the plaintext is processed

- ☞ Block Cipher
- ☞ Stream Cipher

Substitution Ciphers

- A substitution cipher is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns
- uses a key to dictate how the substitution should be carried out.
- Keyword mixed alphabet cipher—Uses a cipher alphabet that consists of a keyword, minus duplicates, followed by the remaining letters of the alphabet
- Simple substitution cipher —Allows any letter to uniquely map to any other letter

CAESAR CIPHERS

- Simplest and earliest known use of a substitution cipher
- Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- Alphabet is wrapped around so that the letter following Z is A
- We simply shift each letter three places to the right in the message to generate the cipher text.
- You can express the rotation 3 (ROT3) cipher in mathematical terms where A is 0 and Z is 25

☞ The encryption function for the Caesar cipher is:

C (P + 3) mod 26

☞ The decryption function is

P (C 3) mod 26

One time Pad

- **A one-time pad** is an extremely powerful type of substitution cipher.
- For a one-time pad encryption scheme to be considered unbreakable, each pad in the scheme must be
  - Made up of truly random values
  - Used only one time
  - Securely distributed to its destination
  - Secured at sender's and receiver's sites
  - At least as long as the message

One time Pad Example

Example

- Message stream 1001010111
- Keystream 0011101010
- Ciphertext stream 1010111101

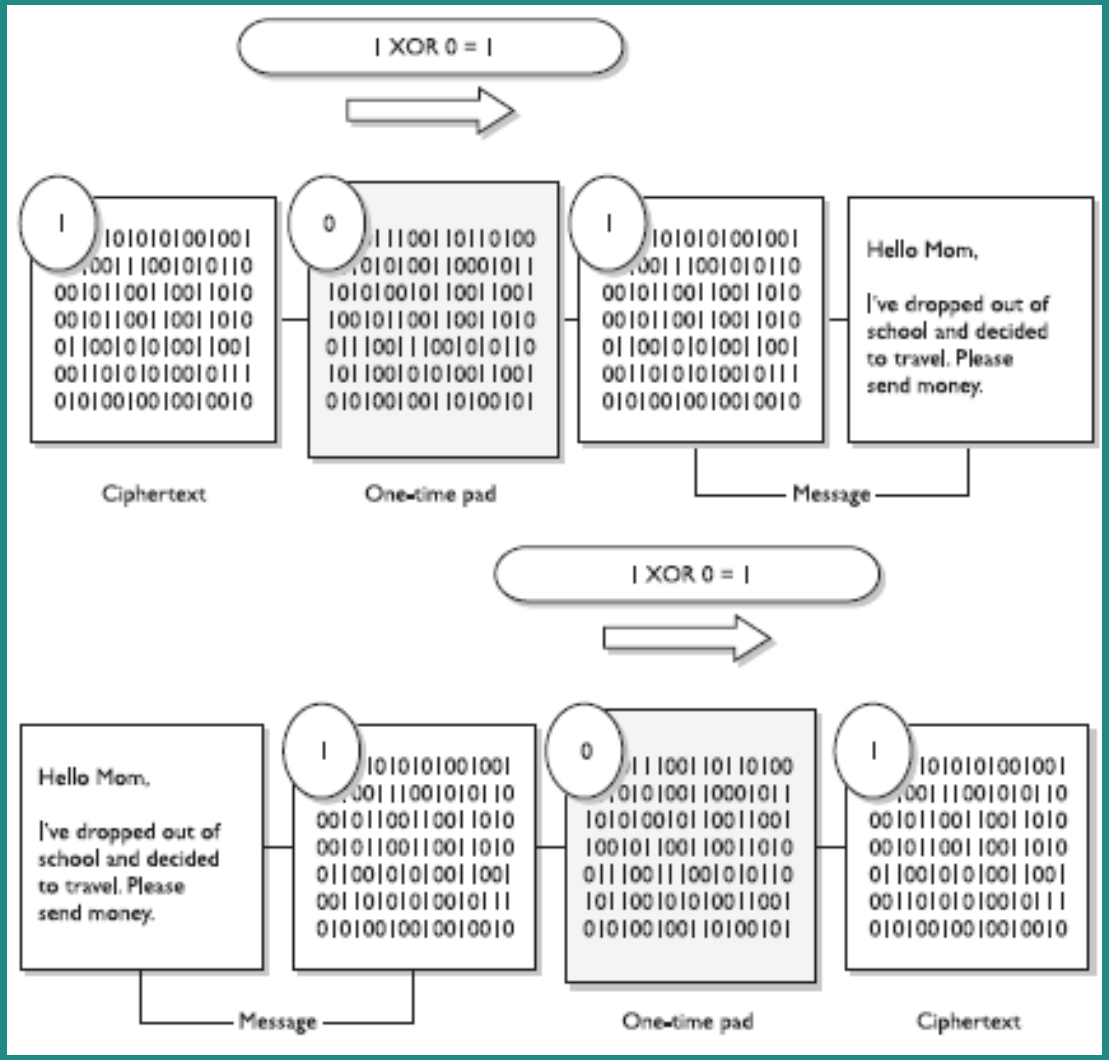
To encrypt:

- The first bit of the message is XORed to the first bit of the onetime pad and so on. The result in the ciphertext value.

To decrypt:

- The receiver takes the first bit of the encrypted message and XORs it with the first bit of the pad. The receiver continues this process for the whole encrypted message, until the entire message is decrypted.

ONE TIME PAD


1 XOR 0 = 1
1
0
1
Hello Mom,
I've dropped out of school and decided to travel. Please send money.
Ciphertext
One-time pad
Message
1 XOR 0 = 1
Hello Mom,
I've dropped out of school and decided to travel. Please send money.
1
0
1
Message
One-time pad
Ciphertext

TRANSPOSITION CIPHERS

- Transposition ciphers use an encryption algorithm to rearrange the letters of a plain-text message, forming the cipher-text message.
- The decryption algorithm simply reverses the encryption transformation to retrieve the original message.
- We can use a keyword to perform a columnar transposition.

TRANSPOSITION CIPHERS

- Message—ATTACK AT DAWN
- Ciphertext—ACDTKATAWATN
- Key— 1,2,3,4

1	2	3	4
A	T	T	A
C	K	A	T
D	A	W	N

TRANSPOSITION CIPHERS EXAMPLE

Example

We're attempting to encrypt the message "The fighters will strike the enemy bases at noon" using the secret key attacker.

1- take the letters of the keyword and number them in alphabetical order. The first appearance of the letter A receives the value 1; the second appearance is numbered 2. The next letter in sequence, C, is numbered 3, and so on.

A	T	T	A	C	K	E	R
1	7	8	2	3	5	4	6

TRANSPOSITION CIPHERS EXAMPLE

Example

We're attempting to encrypt the message "The fighters will strike the enemy bases at noon" using the secret key attacker.

2- Next, the letters of the message are written in order underneath the letters of the keyword

A	T	T	A	C	K	E	R
1	7	8	2	3	5	4	6
T	H	E	F	I	G	H	T
E	R	S	W	I	L	L	S
T	R	I	K	E	T	H	E
E	N	E	M	Y	B	A	S
E	S	A	T	N	O	O	N

TRANSPOSITION CIPHERS EXAMPLE

Example

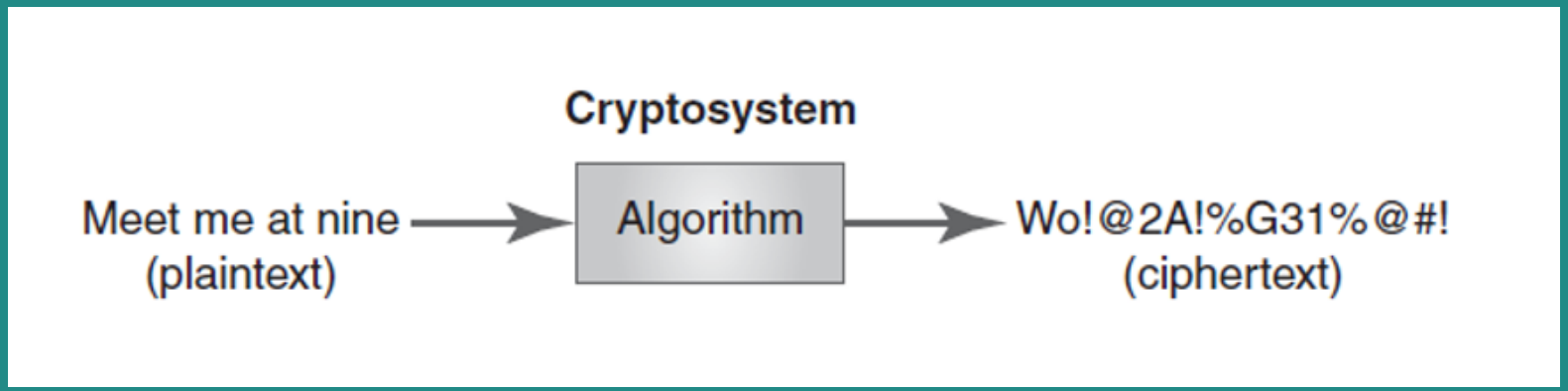
We're attempting to encrypt the message "The fighters will strike the enemy bases at noon" using the secret key attacker.

3- Finally, the sender enciphers the message by reading down each column; the order in which the columns are read corresponds to the numbers assigned in the first step.

```
T E T E E F W K M T I I E Y N H L H A O G L T B O T S E S
  N H R R N S E S I E A
```

A Cryptosystem at Work

- Those that use the same key to encrypt and decrypt are considered a Symmetric encryption
- Those that use different keys to encrypt and decrypt are considered an Asymmetric encryption



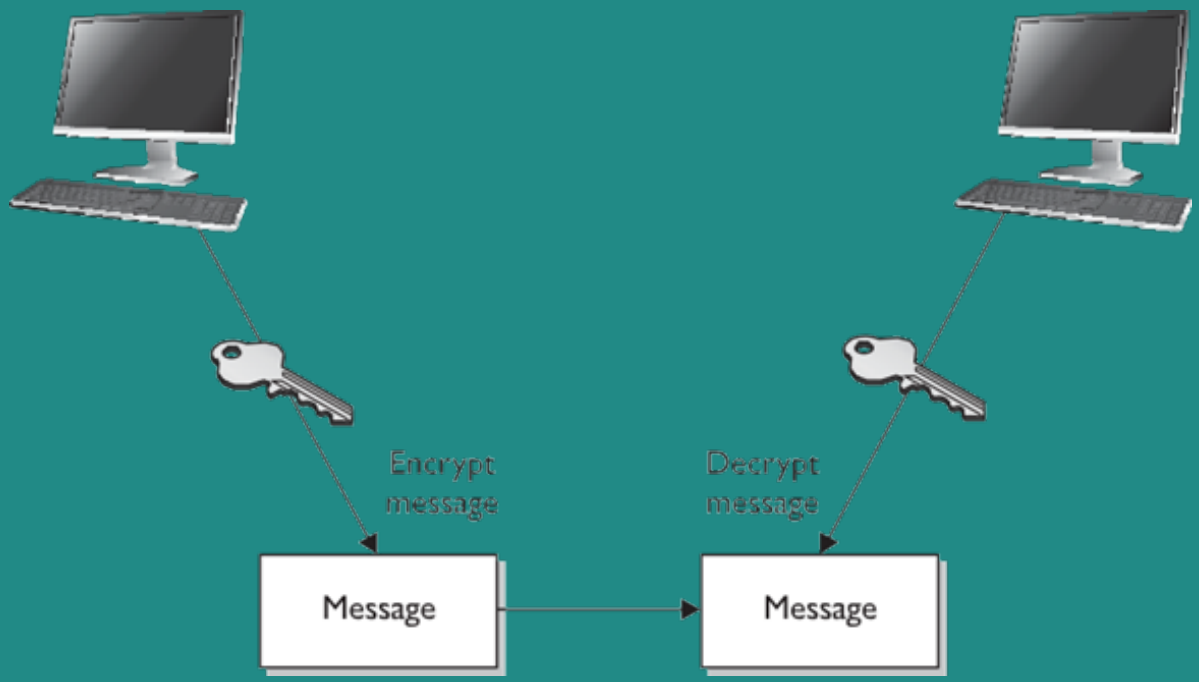
SYMMETRIC ENCRYPTIONS

- In symmetric cryptography the sender and receiver use two instances of the same key for encryption and decryption
- The key has dual functionality, in that it can carry out both encryption and decryption processes.
- Symmetric keys are also called secret keys
  - This type of encryption relies on each user to keep the key a secret and properly protected.
  - If an intruder were to get this key, they could decrypt any intercepted message encrypted with it.
- Each pair of users who want to exchange data using symmetric key encryption must have two instances of the same key.
  - If 100 people were going to communicate, then 4,950 keys would be involved.
  - The equation used to calculate the number of symmetric keys needed is $N * (N - 1)/2$ number of keys

SYMMETRIC ENCRYPTIONS

- The security of the symmetric encryption method is completely dependent on how well users protect the key.
- This should raise red flags for you if you have ever had to depend on a whole staff of people to keep a secret.
- If a key is compromised, then all messages encrypted with that key can be decrypted and read by an intruder.
- Because both users employ the same key to encrypt and decrypt messages, symmetric cryptosystems can provide
  - Confidentiality, but they cannot provide authentication or nonrepudiation.
  - There is no way to prove through cryptography who actually sent a message if two people are using the same key.

SYMMETRIC ENCRYPTION



When using symmetric algorithms, the sender and receiver use the same key for encryption and decryption functions

SYMMETRIC ENCRYPTION STRENGTHS AND WEAKNESSES

- Strengths
  - The major strength of symmetric key cryptography is the great speed at which it can operate.
  - Symmetric keying is very fast, often 1,000 to 10,000 times faster than asymmetric.
  - Symmetric encryption algorithms are also hard to break if a large key size is used.
- Weaknesses
  - Requires a secure mechanism to deliver keys properly.
  - Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming.
  - Provides confidentiality but not authenticity or non-repudiation.

ASYMMETRIC ENCRYPTIONS

- In Asymmetric encryptions sometimes called public key systems each user has two keys:
  - The public key can be known to everyone, and the private key must be known and used only by the owner.
  - The two different asymmetric keys are mathematically related.
  - If a message is encrypted by one key, the other key is required in order to decrypt the message.
- In other words, if the public key encrypts a message, then only the private key can decrypt it, and vice versa.

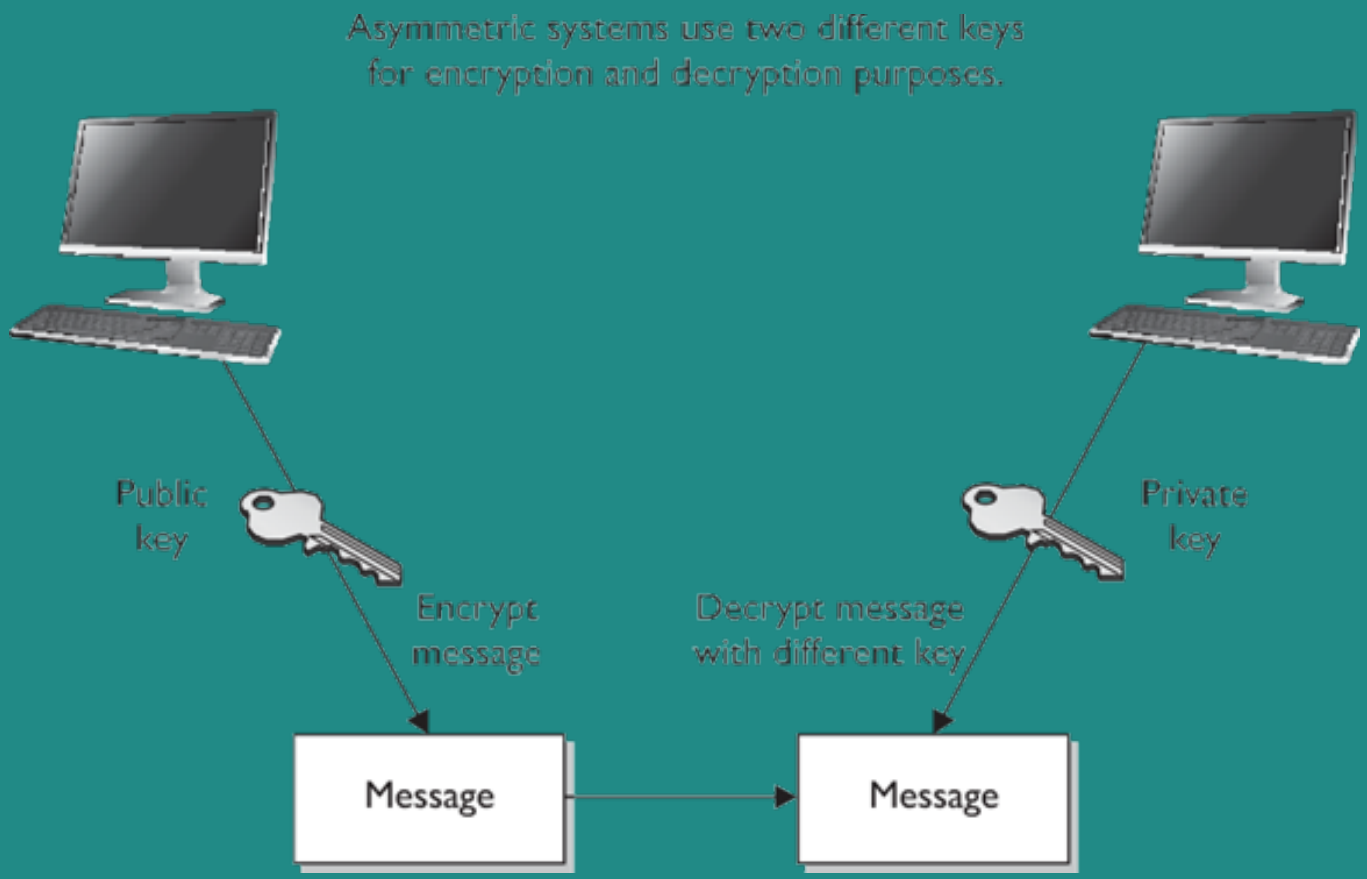
ASYMMETRIC ENCRYPTION FUNCTIONS

- Asymmetric algorithms can provide **authentication** and **nonrepudiation**, depending on the type of algorithm being used.
- Asymmetric systems also provide for easier and more manageable key distribution than symmetric systems and do not have the scalability issues of symmetric systems
- How is **Authentication** provided
  - A message can be decrypted with a public key only if the message was encrypted with the corresponding private key.
  - Bob is the only one who is supposed to have his private key.
  - This provides Authentication

ASYMMETRIC ENCRYPTIONS FUNCTIONS

- How is **Confidentiality** provided
  - ☞ If confidentiality is needed Alice would encrypt the file with the receiver's public key.
  - ☞ This is called a secure message format because it can only be decrypted by the person who has the corresponding private key.
- How is **Non-repudiation** provided
  - ☞ If Alice encrypt the message with her private key.
  - ☞ Only her public key can decrypt it.
  - ☞ Alice cannot deny sending this message if her public key can decrypt it. This is non repudiation

ASYMMETRIC ENCRYPTIONS



An asymmetric cryptosystem

Asymmetric encryption Strengths and weaknesses

- Strengths
  - Better key distribution than symmetric systems.
  - Better scalability than symmetric systems
  - Can provide authentication and non-repudiation
- weaknesses
  - Works much more slowly than symmetric systems
  - Mathematically intensive tasks

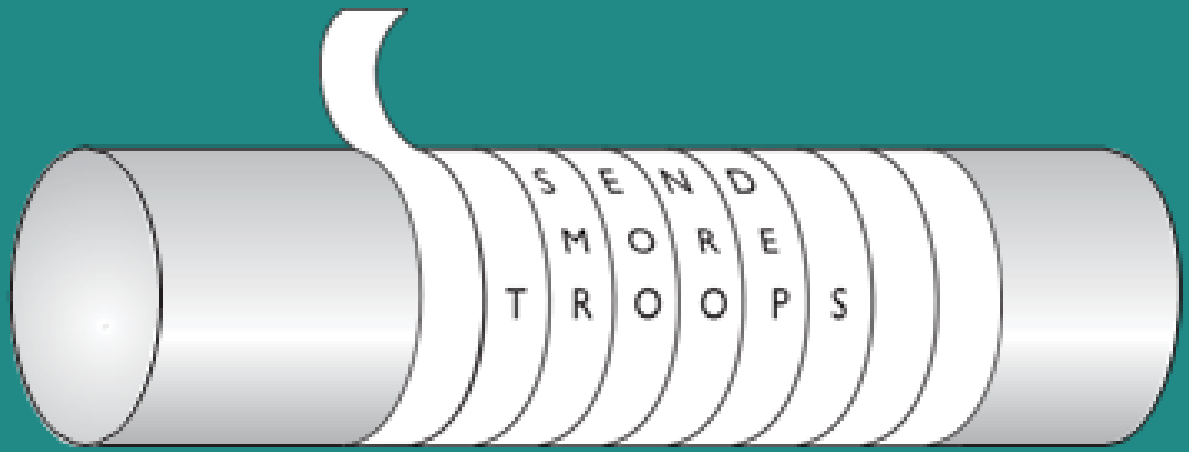
SYMMETRIC AND ASYMMETRIC KEY CRYPTOGRAPHY

Attribute	Symmetric	Asymmetric
Keys	One key is shared between two or more entities.	One entity has a public key, and the other entity has the corresponding private key.
Key exchange	Out-of-band through secure mechanisms.	A public key is made available to everyone, and a private key is kept secret by the owner.
Speed	Algorithm is less complex and faster.	The algorithm is more complex and slower.
Use	Bulk encryption, which means encrypting files and communication paths.	Key distribution and digital signatures.
Security service provided	Confidentiality.	Authentication and nonrepudiation.

Differences Between Symmetric and Asymmetric Systems

CIPHERS

- Cipher systems have long been used by individuals and governments interested in preserving the confidentiality of their communications.
- It's important to remember that these concepts seem somewhat basic, but when used in combination, they can be formidable opponents and cause cryptanalysts many hours of frustration.

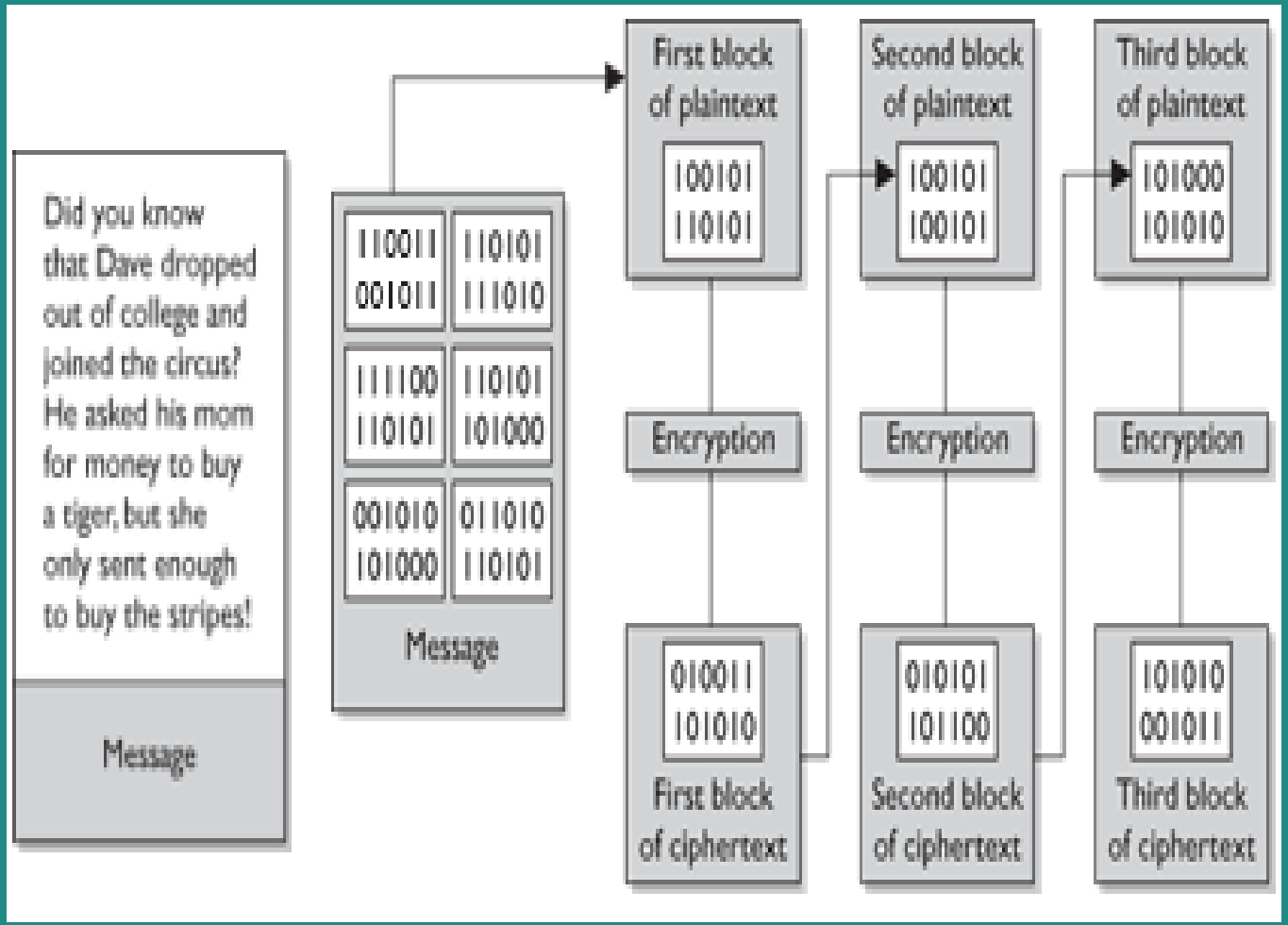


The scytale was used by the Spartans to decipher encrypted messages.

Block Cipher

- Encrypt a block of input to a block of output
- Typically, the two blocks are of the same length
- Most symmetric key systems block size is 64
- In AES block size is 128
- Different modes for encrypting plaintext longer than a block

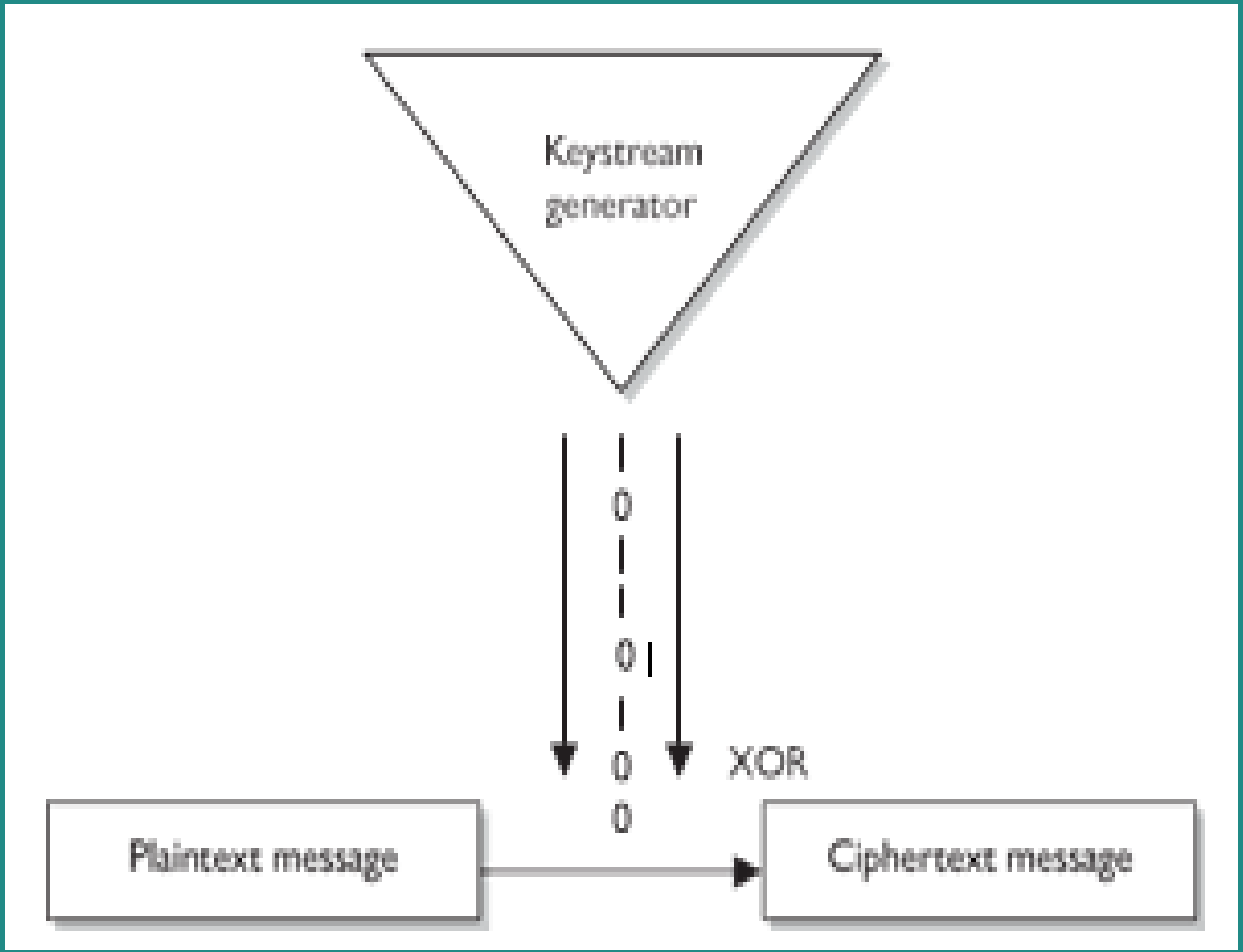
BLOCK CIPHER



STREAM CIPHER

- A stream cipher does not divide a message into blocks.
- A stream cipher treats the message as a stream of bits and performs mathematical functions on each bit individually.
- Stream ciphers use keystream generators, which produce a stream of bits that is XORed with the plaintext bits to produce ciphertext
- Stream cipher is very similar to the one-time pad substitution cipher.

STREAM CIPHER



Putting everything at work

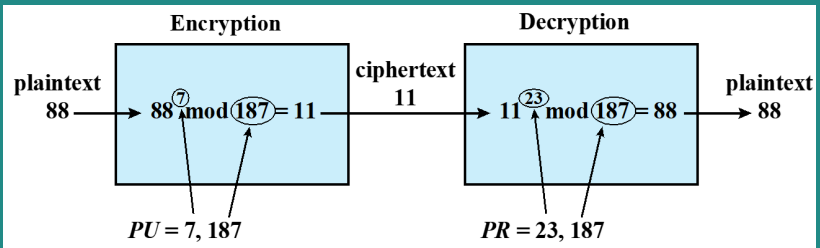
EXAMPLES OF SYMMETRIC ENCRYPTION ALGORITHMS

- DES and Triple-DES are the most common forms of symmetric key block cipher cryptosystems
- Advanced Encryption Standard (AES) was the algorithm eventually chosen to replace DES. It is a block cipher that works on 128-bit blocks. It can have one of three key sizes of 128, 192, or 256 bits.
- This was selected by the United States government to be the replacement for DES and is now the most widely used symmetric key algorithm.

ASYMMETRIC CIPHERS

- RSA (Rivest–Shamir–Adleman) Public key Cryptosystem

have a look at this example online RSA Visual



Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Hashing and Digital Certificates

- The most common hashing functions create the message digest for digitally signed messages
- Hashing is also used to protect user passwords
- Hashing-type functions can also be used with symmetric key cryptography, and the result of the operation is called a message authentication code (MAC)
- Secure Hashing Algorithm (SHA) variants are the most common variants of hashing functions found in commercial software

DIGESTING DATA

- Common hashing algorithms
  - MD5
  - SHA1
- Digital signatures
  - Used to verify the identity of the sender
  - Uses a message digest

Public/Private Key Uses				
	Create digital signature	Verify Digital Signature	Create Digital Envelope	Open Digital Envelope
Sender's private key	X			
Sender's public key		X		
Receiver's public key			X	
Receiver's private key				X

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **Recommended Readings note:** Focus on what was covered in the class. Other parts will come later in other lectures.
  - Chapter 2 , Computer Security: Principles and Practice, , William Stallings and Lawrie Brown
  - Chapter 10, CyBOK, The Cyber Security Body of Knowledge