



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA7028

Data Security and Compliance Week 9 : Cryptography

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Describe dominant InfoSec management models, including national and international standards.
- Explain the importance of access control in InfoSec management.
- Recommend an InfoSec management model and explain how it can be tailored to suit a specific organisation.

Key Concepts

- InfoSec Management Models
- management.
- Access Control
- Key InfoSec Practices

Introduction and Definitions

Cryptography

- **Cryptography** is a method of storing and transmitting data in a form that only those it is intended for can read and process.

Cryptographic systems

- **Cryptographic systems** are a combination of techniques and algorithms that use specific mathematical principles and computations to provide one or more security objectives and goals.

Cryptanalysis

- **Cryptanalysis** are techniques used for deciphering a message without any knowledge of the enciphering details.

Cryptographic process terms



- **Plaintext**—Information in its original and understandable form.
- **Encryption**—The process of scrambling plaintext into ciphertext (or Enciphering).
- **Ciphertext**—Information in scrambled form.
- **Decryption**—The process of unscrambling ciphertext into plaintext (or Deciphering).

Cryptography in Practice

- Cryptography is much more than encryption
 - Hiding data (Steganography)
 - Resisting forgery (Integrity)
 - Resisting unauthorised change (Confidentiality)
 - Resisting repudiation (Non-Repudiation)
 - Enforcing policy (Policies)
 - Exchanging keys (Keys distributions and exchange)

Data states Methods

Data in Transit/Motion

- Protecting data in transit, or when being transported across a network from the risk of interception by encrypting it.

Data at Rest

- Protecting data at rest such as when stored on a hard drive by the use of encryption even when not in use.

Data in Use/Processing

- Data in use, such as when being processed in RAM or CPU registers, is still data that requires protection , and in modern secure systems, this data can be encrypted.

Goals of cryptography

- Security practitioners use cryptographic systems to meet four fundamental goals:
 - Confidentiality
 - Integrity
 - Authentication
 - 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

- Confidentiality in cryptosystems is provided by scrambling the data (Encryption) in a way that can only be read by authorised entity, such as a receiver having the key to descramble (decrypt).
- Secrecy of data is ensured by:
 - Strength of the algorithms
 - Length of the keys
- When Confidentiality is needed in a cryptographic system , we must think about two different types of data:
 - **Data at rest** is that which resides in a permanent location awaiting access.
 - **Data in transit**, or data (in motion or on the wire), is data being transmitted across a network between two systems.

Integrity

- When a message is sent, both the sender and recipient need to know that the message was not altered in transmission
- **Integrity** ensures that data is not altered without authorisation.
 - Message integrity is crucial to message security
 - 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.
 - Important for legal contracts
- **Message integrity** is enforced through the use of encrypted message digests, known as **digital signatures** created upon transmission of a message

Authentication in cryptosystems

- **Authentication** verifies the claimed identity of system users and is a major function of cryptosystems
- Matching of a user to an account through previously shared credentials
 - A combination of cryptographic methods are commonly employed in authentication

Non-Repudiation

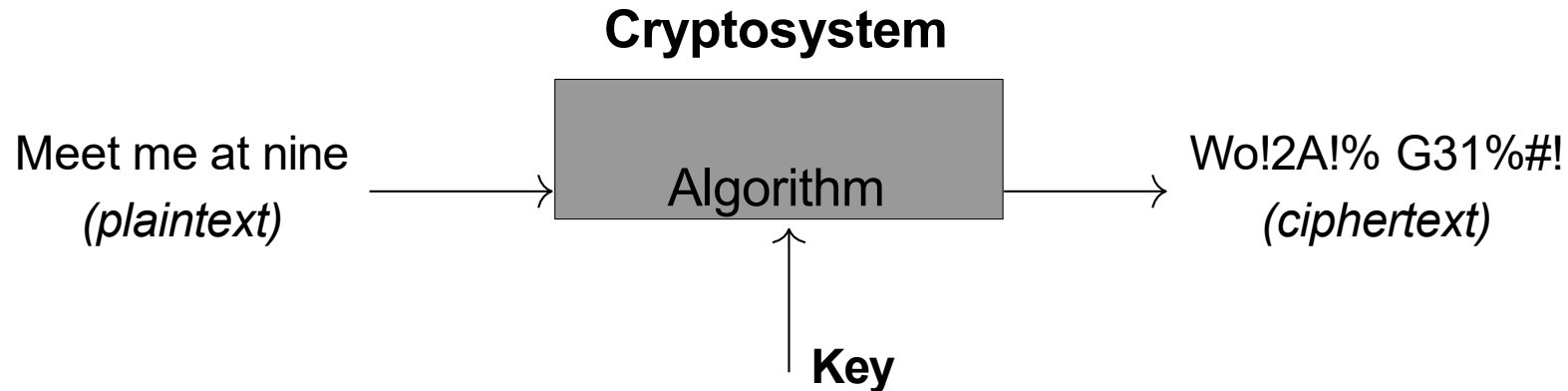
- Non-Repudiation provides assurance to the recipient that the message was originated by the sender and not someone masquerading as the sender.
- The message sender cannot later deny that they sent the message
 - Important in electronic exchanges of data because of the lack of face-to-face meetings
- It also prevents the sender from claiming that they never sent the message in the first place (also known as repudiating the message).

Cryptosystems components

Cryptosystems

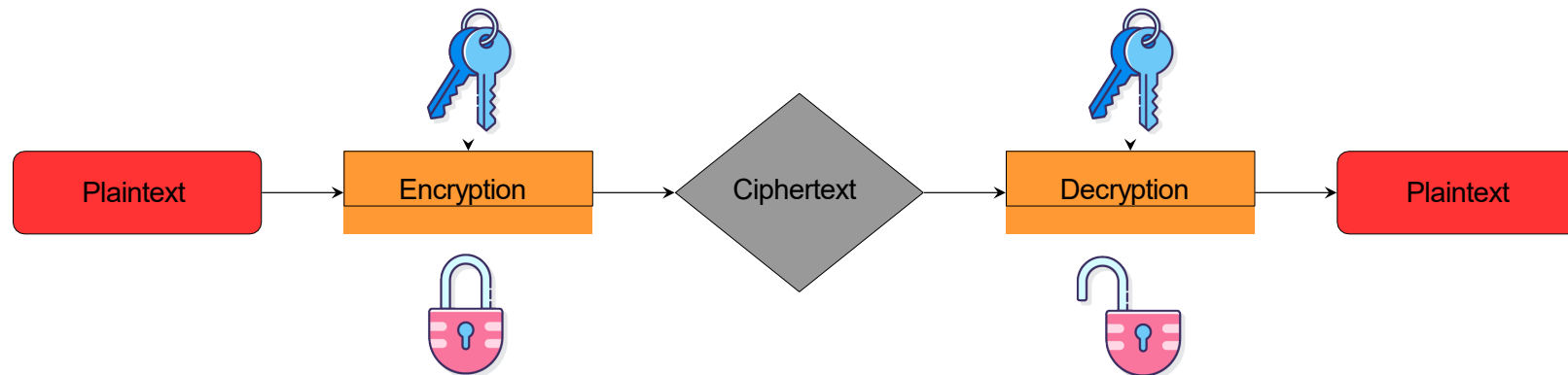
A **cryptosystem** encompasses all of the necessary components for encryption and decryption to take place.

- Software
- Algorithms
- Protocols
- Keys



Modern Cryptographic algorithms

- Modern Cryptographic algorithms are built around complex mathematical functions that combines various operations and methods of how the plaintext is processed with various randomness operations to produce a strong cryptography algorithm.
- Specific properties make them resistant to reversing or solving by means other than the application of the algorithm and key



While everyone knows how to use a open the lock, without the key to unlock the lock, that knowledge is useless.

Cryptographic Systems

- A cryptographic system is characterised along three independent dimensions:
 - The type of operations used for transforming plaintext to ciphertext, which can perform either **Confusion, Diffusion**, or both.
 - Substitution: replacing an item with a different item
 - Transposition: changing the order of items
 - The way in which the plaintext is processed
 - block Cipher
 - Stream Cipher
 - The number of keys used:
 - Symmetric- and Asymmetric
- In addition to these dimensions, there is a unique method to hide information called **Steganography** .

Confusion and Diffusion

- Cryptographic algorithms rely on two basic operations to transform and to obscure plaintext messages: confusion and diffusion.
- Confusion occurs when the relationship between the plaintext and the key is so complex that an attacker cannot easily alter the plaintext and analyse the resulting ciphertext to determine the key.
- Diffusion occurs when a change in the plaintext results in multiple, widespread changes throughout the ciphertext.

Substitution Ciphers Operation

- A substitution cipher is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- This is considered a form of confusion because the plaintext characters are now obscured in the ciphertext.
- The plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns
- A simple substitution cipher allows any letter to uniquely map to any other letter

Substitution Ciphers Operation

- Romans typically used a shift cipher (Rotation)
 - A modern-day example of a shift cipher is the ROT13 cipher, where every letter is rotated 13 positions in the alphabet. For example a becomes n, b becomes o.
- Caesar's cipher is another shift cipher
 - Algorithm specifies an alphabet offset either to the right (forward) or to the left (backward); the key specifies the number of letters in the offset
 - Both methods uses same formulas to encrypt or decrypt
 - Forward offset- **Encrypt** $C = (P - K) \bmod 26$, **Decrypt** $C = (P - K) \bmod 26$
 - Roman is only forward offset rotation
 - Caesar can also be Backward offset rotation- **Encrypt**
 - $C = (P - K) \bmod 26$, **Decrypt** $C = (P - K) \bmod 26$

Substitution Cipher Operation



Any shift cipher can easily be encoded and decoded on a wheel of two pieces of paper with the alphabet set as a ring; by moving one circle the specified number in the shift, you can translate the characters. ROT19

transforms the character A to become T

*Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives*

Polyalphabetic substitution Cipher Operation

- The Vigenere cipher works as a polyalphabetic substitution cipher that depends on a password.
- The Vigenere cipher is a more complex substitution cipher that allows letters to map to another letter by the use of substitution table . The process involves:
 - For encryption:
 - i. Identify the **plaintext character from the row.**
 - ii. Identify the **keystream character from the column.**
 - iii. Find the **intersection of the row and column** to get the **ciphertext** character.
 - For decryption:
 - i. Identify the **keystream character from the column.**
 - ii. Identify the **ciphertext character** from the **row of the keystream character column.**
 - iii. **Trace back to the plaintext character** at the start of the **row.**

Polyalphabetic Substitution Cipher Operation

		Keystream																											
Plaintext		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z		
	a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	
	b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	
	c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	
	d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	
	e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	
	f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	
	g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	
	h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	
	i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	
	j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	
	k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	
	l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	
	m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	
	n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	
	o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	
	p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	
	q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	
	r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	
	s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	
	t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	
	u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	
	v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	
	w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	
	x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	
	y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	
	z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	

PlainText	M	E	s	S	A	G	E	S
KeyStream	P	A	S	S	W	O	R	D
CipherText	B	E	K	K	W	U	V	V

Transposition Cipher Operation

- 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.

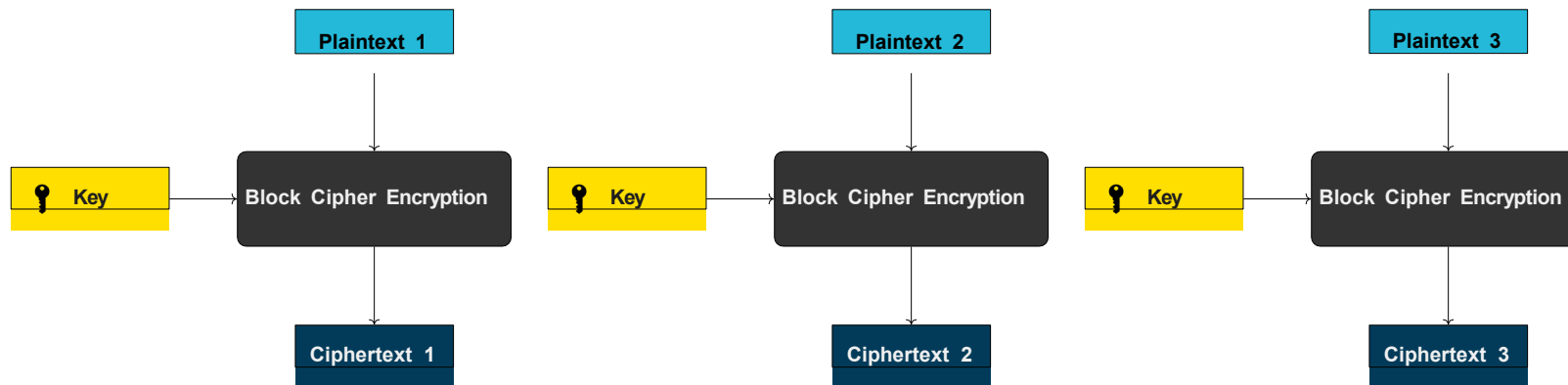
		The secret message: "Attack at dawn"			
Step 1	1- Write the Secret keyword cats	c	a	t	s
	2- Put a number below each letter by the order it appears in the alphabet	↓	↓	↓	↓
		2	1	4	3
Step2	3- Write the secret message horizontally , the message using the length of the actual keyword. Create as many rows as you need	a	t	t	a
		c	k	a	t
		d	a	w	n
Step 3	4- Read vertically the letters, in the order of the columns identified in Step 1 . This is the cipher text.	2	1	4	3
		↓	↓	↓	↓
		a	t	t	a
Step 4	The cipher text is: "tkaacd at ntaw"	c	k	a	t
		d	a	w	n

Ciphers

- Cipher systems have long been used by individuals and governments interested in preserving the confidentiality of their communications.
- In addition to how the data is scrambled to ensure secrecy, another dimension of Cryptography focuses on how the data is processed.
- There are two methods in cryptography to process the data in a cryptographic algorithm. The methods are:
 - Block Cipher
 - Stream Cipher
- 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.

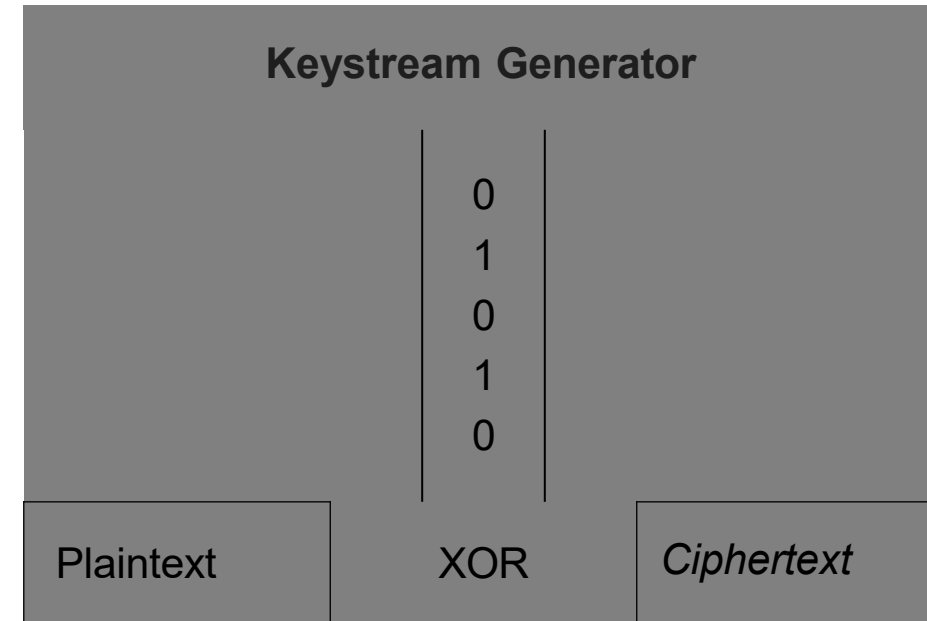
Block Cipher

- 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
- Block cipher has different modes for encrypting plaintext longer than a block



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

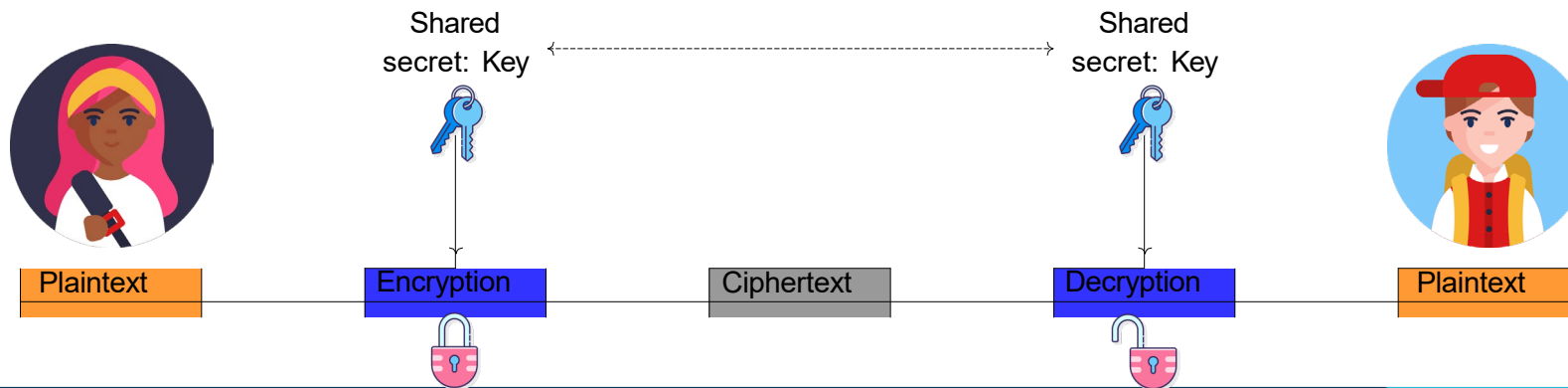


Cryptographic Functions and Ciphers

- 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.
- Three types of commonly used encryption algorithms
 - Symmetric algorithms use the same key for encryption and decryption
 - Asymmetric algorithms employ two keys, a public key and a private key, making up what is known as a key pair

Symmetric encryptions

- In symmetric cryptography the sender and receiver use two instances of the same key for encryption and decryption
- Symmetric encryptions examples are Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Triple DES (3DES)
- Symmetric keys are also called shared secret keys.
 - If 100 people were going to communicate, then 4950 pair of keys would be involved.



Symmetric encryptions

- Symmetric encryption relies on each user to keep the key a secret and properly protected.
- It is completely dependent on how well users protect the key.
 - Must be a mechanism for key management such as key distribution and key revocation.
- If an intruder were to get this key, they could decrypt any intercepted message encrypted with it.
- Symmetric cryptosystems can provide Confidentiality:
- Symmetric cryptosystems cannot provide authentication or Non-Repudiation.
 - There is no way to prove through cryptography who actually sent a message if two people are using the same key.

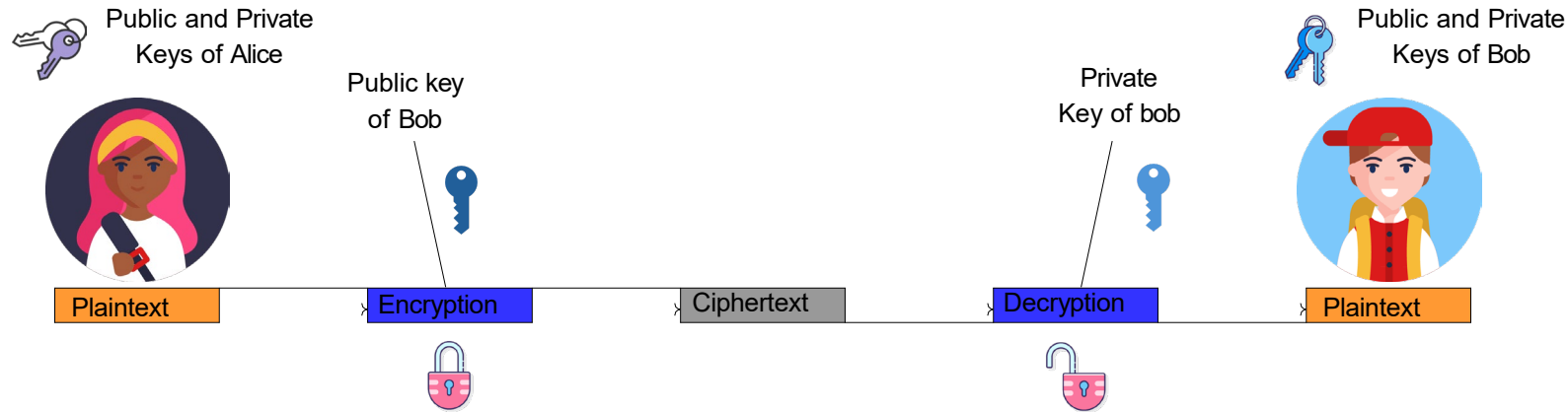
Symmetric encryption algorithms

- DES (Data Encryption Standard)
 - Was widely used in the 1970s–1990s for government and commercial encryption.
- 3DES (Triple DES)
 - More secure than DES but now considered slow and outdated; being phased out.
- AES (Advanced Encryption Standard)
 - Highly secure and efficient
 - widely adopted for modern encryption (e.g., Wi-Fi, VPNs, file encryption).
 - The current encryption standard recommended by NIST.

Asymmetric encryptions

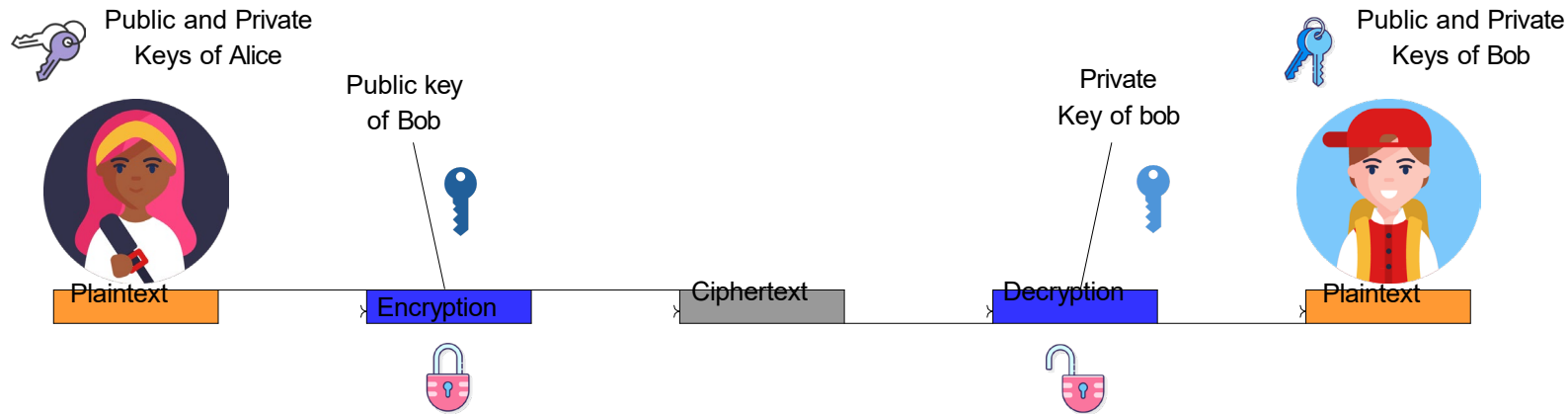
- In Asymmetric encryptions sometimes called public key systems each user has two keys:
 - The public key can be known to everyone, and the private key must be known and used only by the owner.
 - The two different asymmetric keys are mathematically related.
 - In other words, If a message is encrypted by one key, the other key is required in order to decrypt the message.
- Each user using an asymmetric encryption algorithm needs their own pair of keys containing one public key and one private key.
 - If 100 people were going to communicate, then 200 keys or 100 pair of keys would be involved.
- Asymmetric systems also provide for easier and more manageable key distribution than symmetric systems and do not have the scalability issues of symmetric systems.

Asymmetric encryption functions



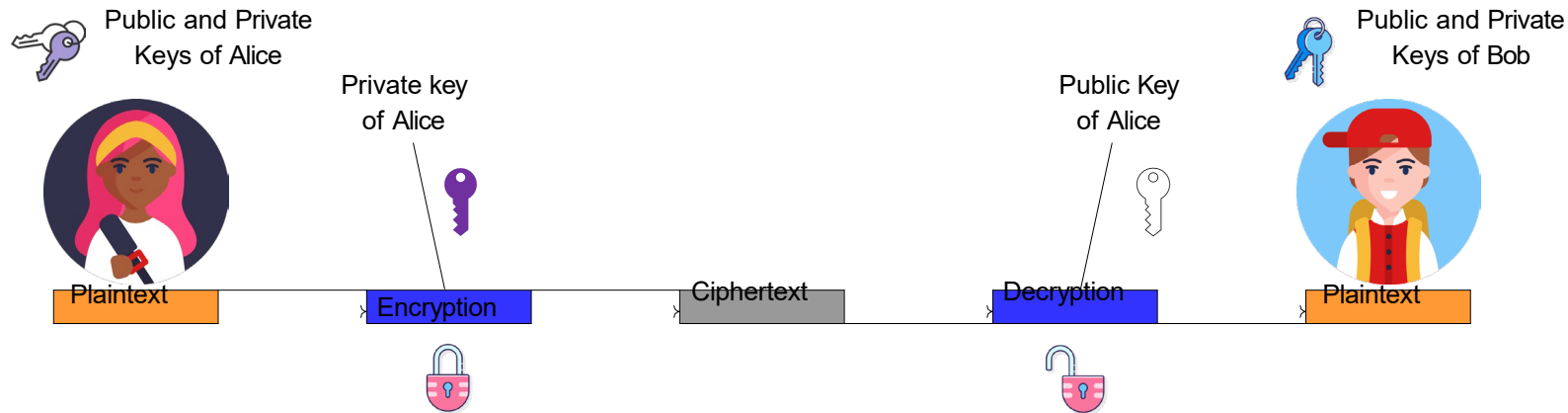
- How **Confidentiality** is provided in asymmetric encryption:
 - If confidentiality is needed Alice would encrypt the file with the receiver's public key.
 - This is called a secure message format because it can only be decrypted by the person who has the corresponding private key.

Asymmetric encryption functions



- How **Authentication** is provided in asymmetric encryption:
 - 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 encryption functions



- How the **Non-repudiation** function provided in asymmetric encryption:
 - 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 encryption algorithms

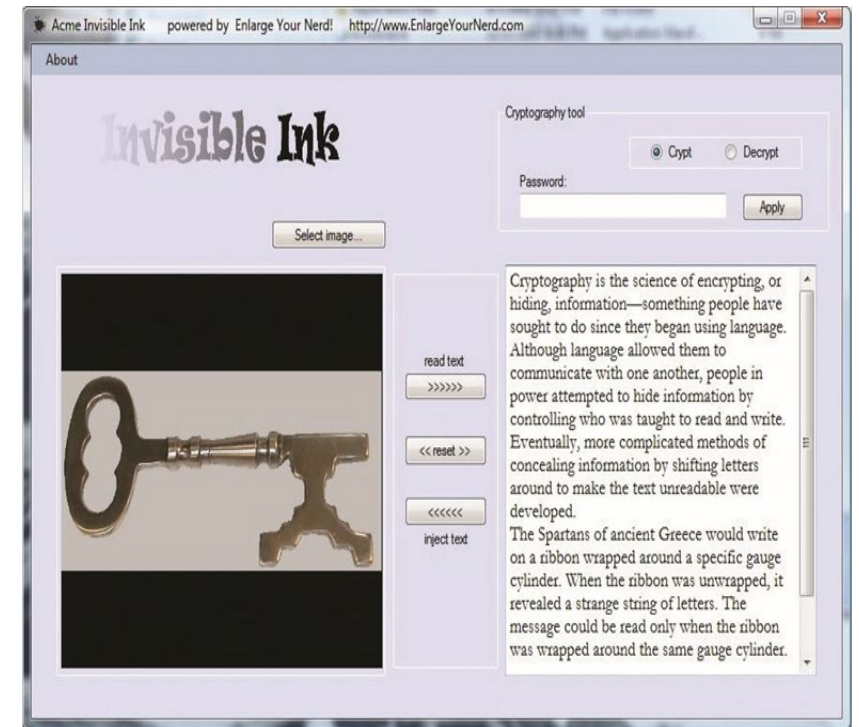
- RSA (Rivest–Shamir–Adleman)
 - One of the most widely used public key algorithms.
 - Based on the difficulty of factoring large prime numbers.
- ECC (Elliptic Curve Cryptography)
 - Uses properties of elliptic curves over finite fields.
 - Offers strong security with smaller key sizes compared to RSA.
 - Popular in mobile and embedded systems.

Steganography

- Steganography is a method of hiding data in another media type so the very existence of the data is concealed- **Security through Obscurity**.
- The message is not encrypted, just hidden.
- Only the sender and receiver are supposed to be able to see the message because it is secretly hidden in a graphic, audio file, document, or other type of media.
- Media files are ideal for steganographic transmission because of their large size.
- 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.
 - Encrypted messages can draw attention because they tell malicious actors that you have sensitive data therefore you are encrypting them.

Detecting Steganography

- Most publicised uses of steganography are to hide illegal material
 - Covert communication by terrorist networks
- Detection is difficult
 - Messages do not attract attention
 - Data can also be encrypted
- There are many tools to detect steganography i.e- invisible Ink, Stegdetect, StegSecret and StegSpy



Steganography detection by Invisible Ink tool

Hashing Functions

- A hash (or hashing) function is a special mathematical function that performs a **one-way function**
 - Once the algorithm is processed, there is no feasible way to use the ciphertext to retrieve the plaintext
 - There is no feasible way to generate two different plaintexts that compute to the same hash value
- it is used in cryptography to:
 - Store computer passwords
 - Ensure message integrity
- Hashing produces a unique value
 - Corresponds to the data entered
 - The hash output , called **Message digest** or the **Hash**, is also reproducible by anyone else running the same algorithm against the same data

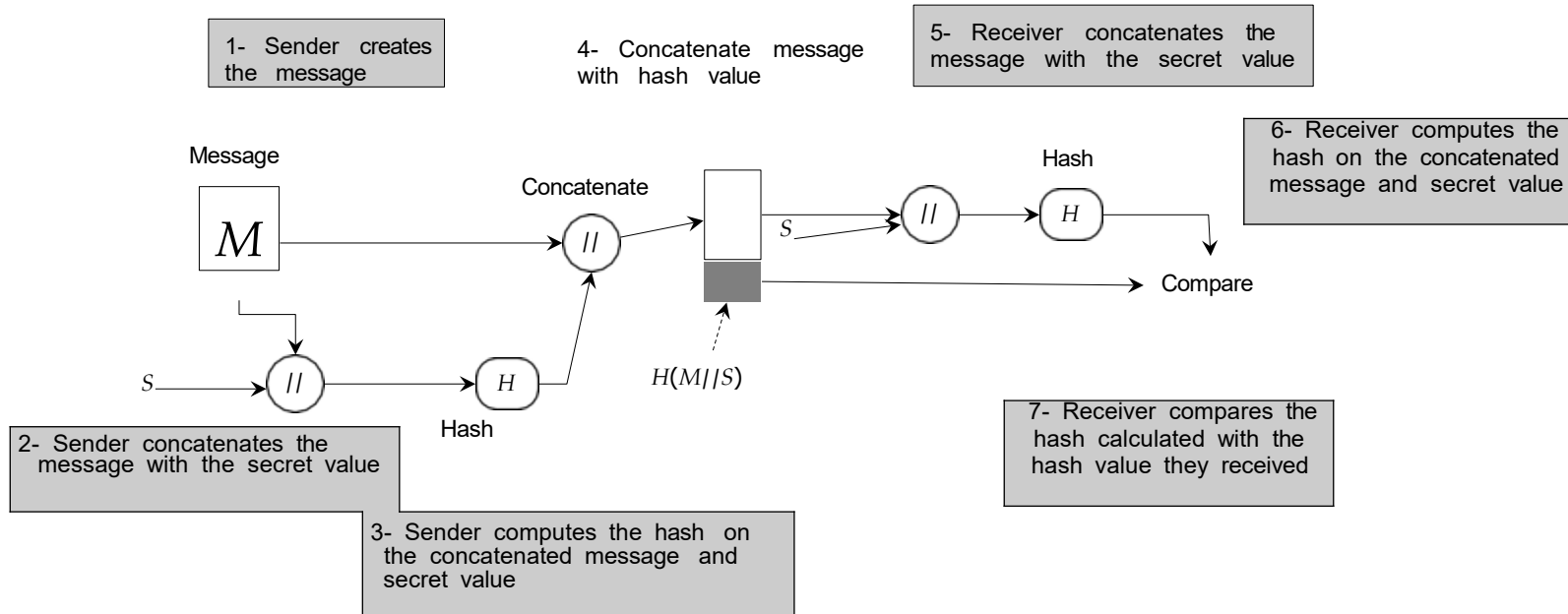
Hash Function and Integrity

- Hash functions:
 - Help detect forgeries
 - Compute a checksum of a message
 - Combine the checksum with a cryptographic function so that the result is tamper-proof
- A hash is:
 - A checksum designed so that no one can forge a message in a way that will result in the same hash as a legitimate message
 - Usually a fixed size, resulting in a hash value, which is larger than checksum values

Message Authentication Code (MAC)

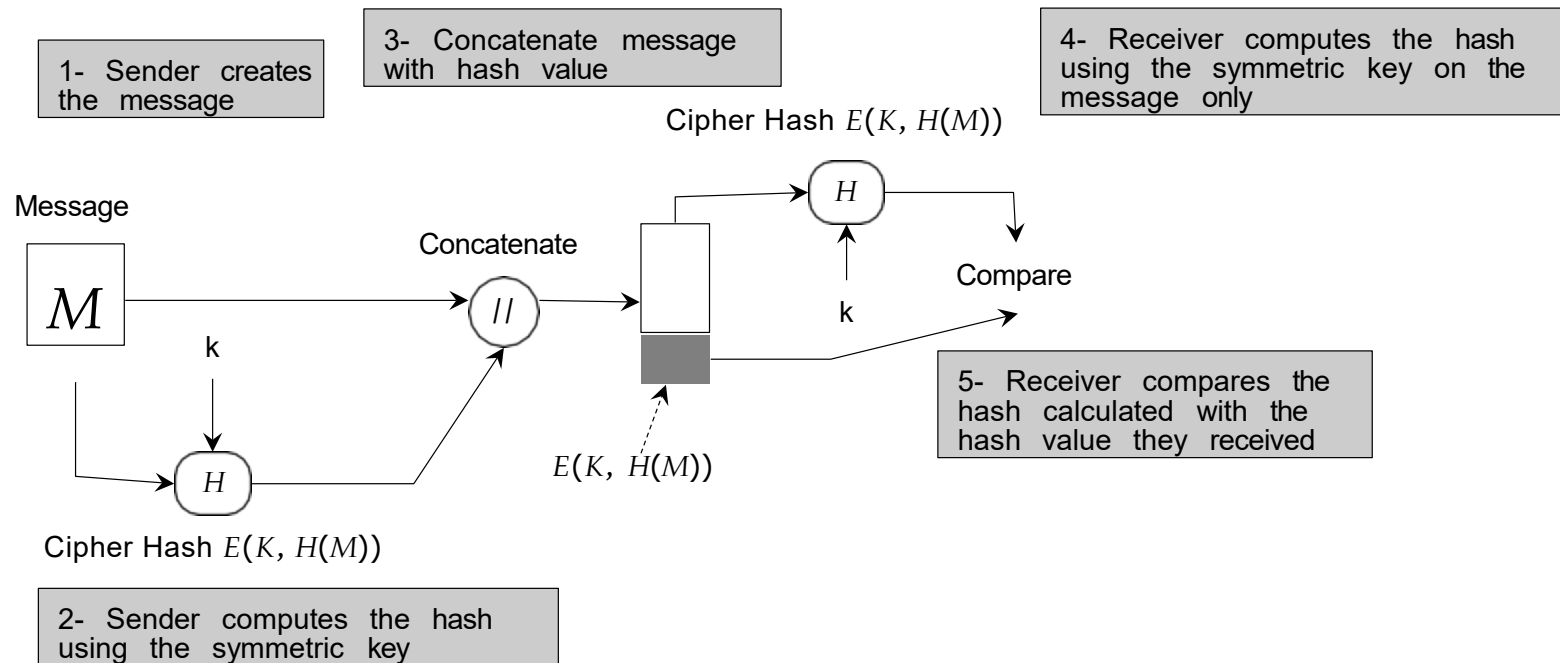
- Also known as a keyed hash function
- Typically used between two parties that share a secret key to authenticate information exchanged between those parties
- MACs are often generated using either a hash function called (HMAC) or a cryptographic algorithm called (CMAC)
- Takes as input a secret key and a data block and produces a hash value (MAC) which is associated with the protected message
 - If the integrity of the message needs to be checked, the MAC function can be applied to the message and the result compared with the associated MAC value
 - An attacker who alters the message will be unable to alter the associated MAC value without knowledge of the secret key

HMAC



A computes the hash value using a standard hashing function such as MD5 or SHA over the concatenation of M and S and appends the resulting hash value to M . Because B possesses S , it can recompute the hash value to verify the authenticity of the message using the same hash function. Because the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message. Ensures authentication, and integrity.

CMAC



The hash code is computed using symmetric encryption. This reduces the processing burden for those applications that do not require confidentiality and only require to protect the integrity. Decryption is not even needed.

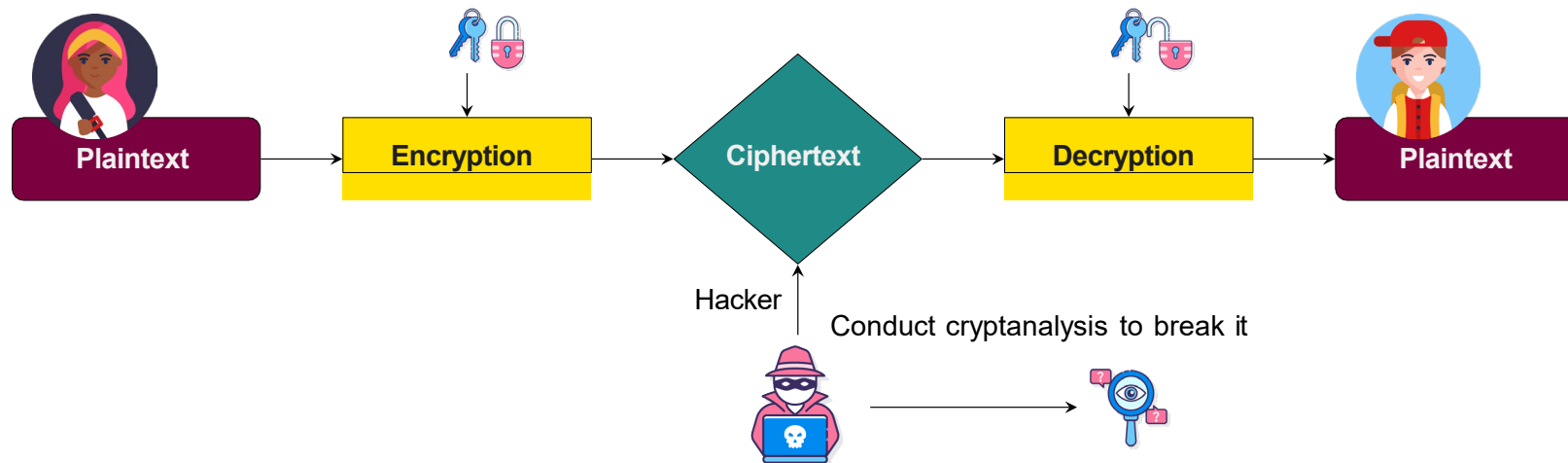
Ensures authentication, and integrity.

Post Quantum cryptography

- A branch of cryptography focused on developing algorithms that are resistant to quantum computer attacks.
- Traditional algorithms like **RSA**, **DSA**, and **ECC** are vulnerable to Shor's algorithm, which quantum computers can use to break them.
- Advantages:
 - Future-proofing sensitive data against quantum threats.
 - B. Resistance to attacks from quantum computers

Cryptanalysis

- Cryptanalysis is the process of analysing available information in an attempt to return the encrypted message to its original form
- The objective is to break cryptographic security systems and gain access to the contents of encrypted messages, without necessarily having access to the secret key used to encrypt the messages.
- Many Cryptanalysis methods are used by hackers and cybersecurity experts to decipher encrypted data in modern cryptography.



Cryptanalysis methods

- **Differential cryptanalysis** - Compares input plaintext and output ciphertext to determine the key
- **Collision attack**: Two different inputs result in the same output
- **Brute Force** Tries every possible key until found.
- **Dictionary Attack** Uses a list of common words, phrases, and previously leaked passwords to attempt to guess a password.
- **Frequency and pattern analysis**: Analyses the frequency of characters or patterns to deduce the key.
- **Downgrade attack**: Attacker takes advantage of backward compatibility in some algorithms, to downgrade the security.
- **Known Plaintext Attack**: If the attacker has access to both the plaintext and its ciphertext, they might be able to deduce the key.
- **Quantum Computing** poses a potential future threat to traditional cryptographic algorithms, as it could theoretically break many of the current encryption methods.

References

- All slides are my own.
- You can read about cryptography in the recommended books:
 - Chapter 10, Whitman, M.E., Mattord, H.J., Principles of Information Security . Cengage Learning 658.



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk