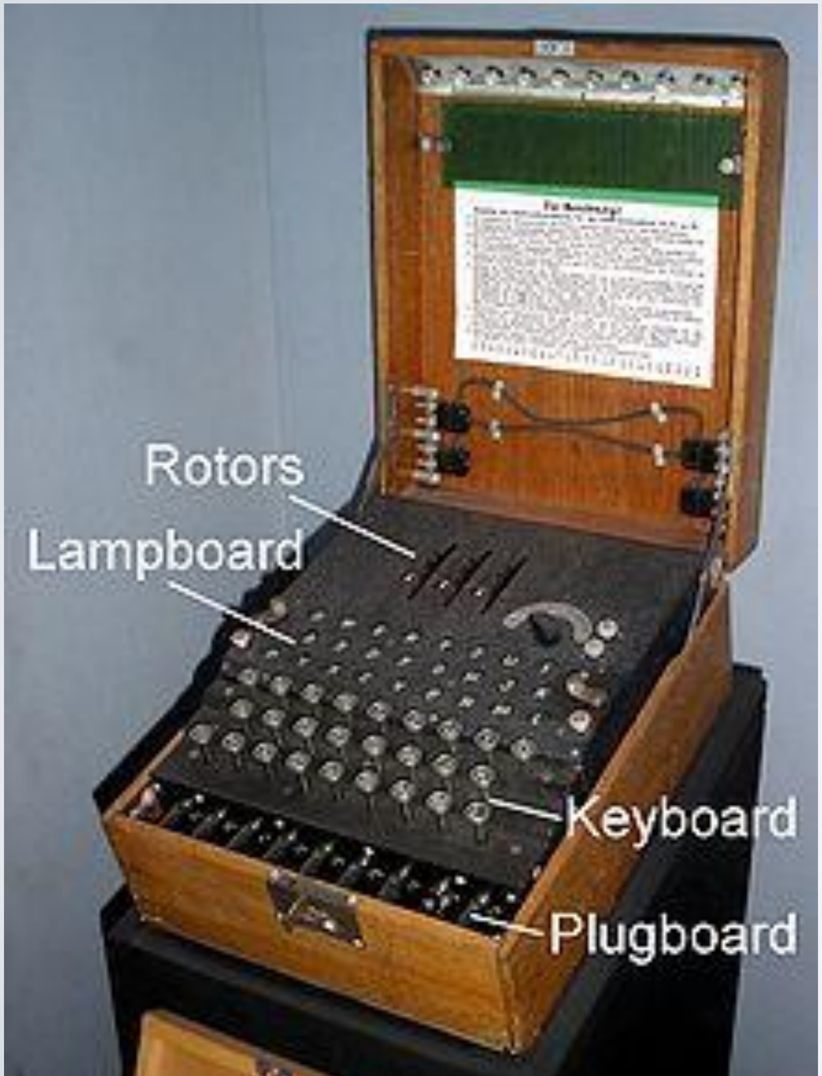
UNIVERSITY OF PLYMOUTH

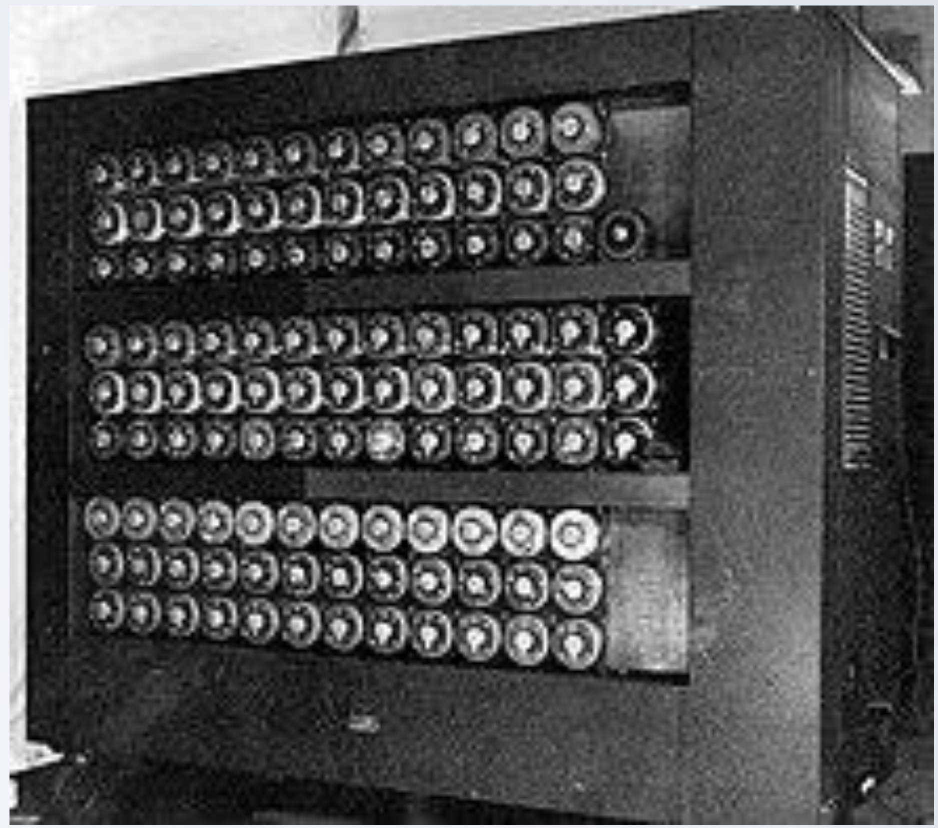
Cryptography

Dr Hai-Van Dang

Centre for Security, Communications and Network Research

What are these machines?





Learning outcome checklist

- LO1: Recognize cryptographic techniques
- LO2: Encrypt/ decrypt a message with symmetric encryption
- LO3: Encrypt/ decrypt a message with public key encryption
- LO4: Calculate hash value and use it
- LO5: Calculate Message Authentication Code and use it
- LO6: Sign/ verify a message
- LO7: Cryptanalyse (decipher)

Further reading

- LO1, LO2, LO7: Martin, K.M. (2017), Everyday Cryptography: Fundamental Principles and Applications – section 2.1.1, 2.1.2
- LO3: https://www.youtube.com/watch?v=GSIDS_lvRv4
- LO4: https://www.youtube.com/watch?v=8ZtInClXe1Q, https://www.youtube.com/watch?v=b4b8ktEV4Bg
- LO5: https://www.youtube.com/watch?v=MKn3cxFNN1I
- LO6: https://www.youtube.com/watch?v=s22eJ1eVLTU

Session Content

Principles & Terminology

Cryptographic Algorithms

Applied Cryptography

Key Distribution

Cryptanalysis

Conclusions

Principles and Terminology

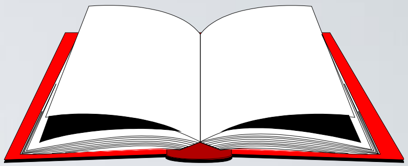
Introduction

- Transformation of information into an encrypted form that cannot be read by third parties
- Originally used almost exclusively for diplomatic and military communications
  - fundamental change due to public / commercial use of IT-based communications
- May be applied to data communications or stored information

Examples of data communication threats

- Interception
  - A message may be obtained and read by a third party, thus affecting *confidentiality*
- Modification or substitution
  - A message could be altered or entirely replaced, thus affecting *integrity*
- Blocking
  - Someone may attempt to block a communication, thus affecting the *availability* of the data

Terminology



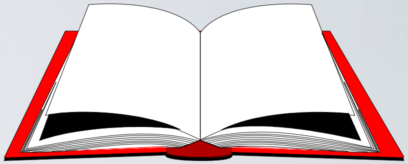
- **Plaintext**
  - the readable message or data which will be used by the cryptographic process

The quick brown fox jumped over the lazy dog

- **Ciphertext**
  - the un-readable message or data which is the outcome of the cryptographic process

%4kigi^5js89t-hlvkn
Jp0”390\<0#;e,843of
9=2

Terminology



- **Encryption** [enciphering]
  - encryption is the process of turning plaintext into ciphertext
- **Decryption** [deciphering]
  - decryption is the process of turning ciphertext into plaintext.

Terminology

- **Cryptography**
  - a cipher system where plaintext is transformed into ciphertext using an algorithm
  - at the recipient end, the message is deciphered to recover the original
- **Cryptanalysis**
  - used by an interceptor on the ciphertext to determine the plaintext information
- **Cryptology** = Cryptography + Cryptanalysis

Cryptographic Algorithms

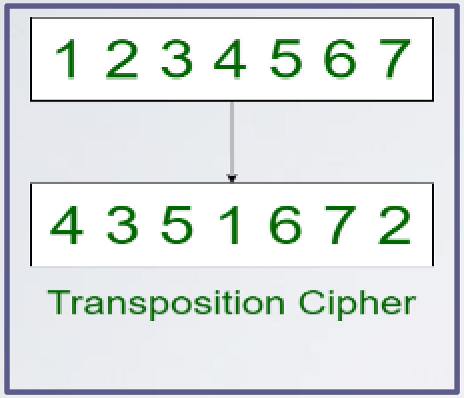
Implementing Cryptography

- Simplest arrangements rely on secrecy of the cryptographic algorithm
  - once discovered all the information is insecure

- Security improved by using a key :
  - constant algorithm, but produces different output depending on key value
  - key can be changed if compromise suspected
  - Number of possible keys = ‘key space’
  - problem with key distribution - require secure protocols

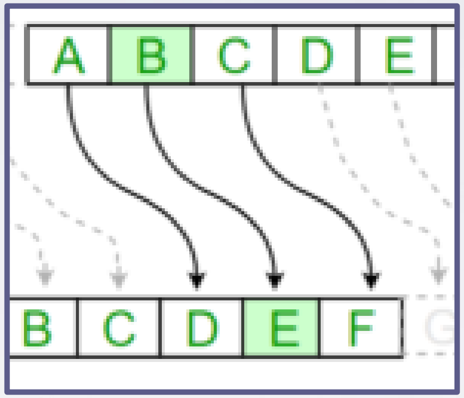
Basic Cryptographic Techniques

Transposition



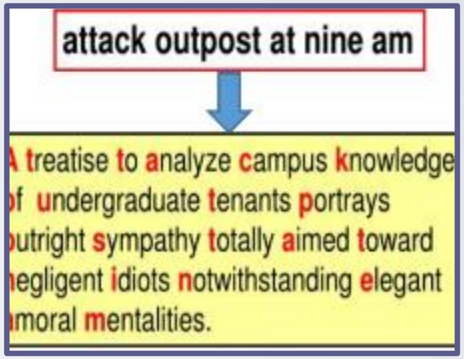
Symbols in the plaintext are **moved** into different positions in the ciphertext.

Substitution



Symbols in the plaintext are **replaced** with different (usually) symbols in the ciphertext.

Concealment



Additional symbols are placed in the ciphertext to conceal the content.

https://www.geeksforgeeks.org/difference-between-block-cipher-and-transposition-cipher/
https://www.geeksforgeeks.org/substitution-cipher/
https://slideplayer.com/slide/6100284/ (slide 3)

Cryptographic Techniques

- Transposition
  - the method by which symbols in the plaintext are moved into different positions in the ciphertext.
- Substitution
  - the method by which symbols in the plaintext are replaced with different (usually) symbols in the ciphertext.
- Concealment
  - the method by which additional symbols are placed in the ciphertext to conceal the content.

Cryptographic Techniques
Transposition

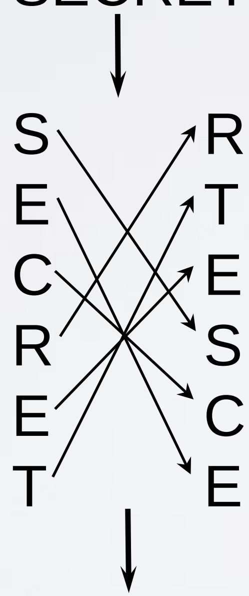
- Rearrangement of the order of bits in a data block according to a fixed permutation
- Only secure if each message has its own transposition
- Simple transposition may be target of brute force attack :
    - attempting each permutation of encrypted text

Transposition Methods

Simple transposition

Plaintext: SECRET

Encrypt:



Ciphertext: RTESCE

Transposition using matrix

Plaintext: THISISASECRETMESSAGE

Encrypt:

T	H	I	S	I
S	A	S	E	C
R	E	T	M	E
S	S	A	G	E

Ciphertext: TSRSHAESISTASEMGICEE

Exercise

1. Encrypt the below plaintext using Matrix Transposition encryption with 4 columns

YOU ARE GOOD

(if the matrix is not full, using X as padding/ to fill up the matrix)

2. Decrypt the below ciphertext using Matrix Transposition encryption with 4 columns

GDOAOYDX

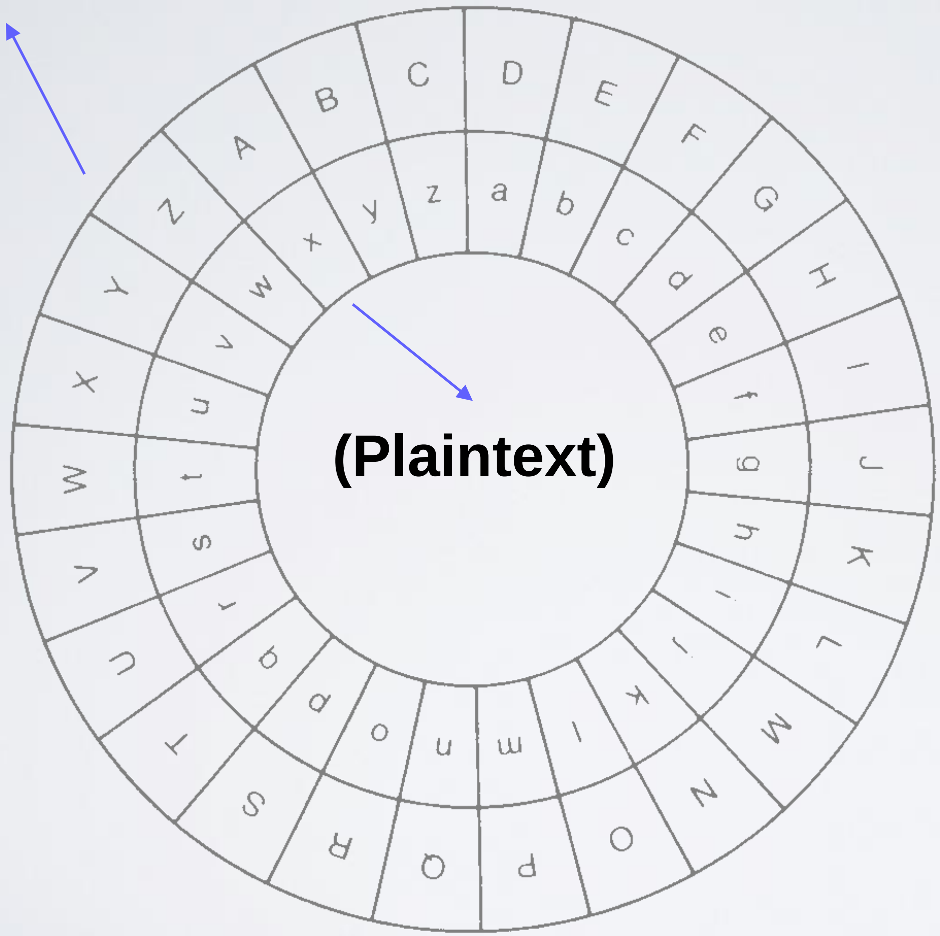
(if there is any X at the end of the plaintext, it is the padding that could be removed)

Cryptographic Techniques
Substitution

- Systematic replacement of one symbol by another (monoalphabetic cipher)
- Uses a lookup table
- Vulnerable to statistical analysis
  - e.g. based upon frequency of character occurrence
- E.g. Caesar Cipher (3 place offset in alphabet)

Example of Substitution

(Ciphertext)



(Plaintext)

secretmessage

Encrypt

VHFUHWPHVVDJH

(Ciphertext)

$$c_i = E(p_i) = p_i + 3$$

Exercise

1. Encrypt the below plaintext using Caesar cipher with key K=4

YOU ARE GOOD

2. Decrypt the below ciphertext using Caesar cipher with key K=2

UVCA YGNN

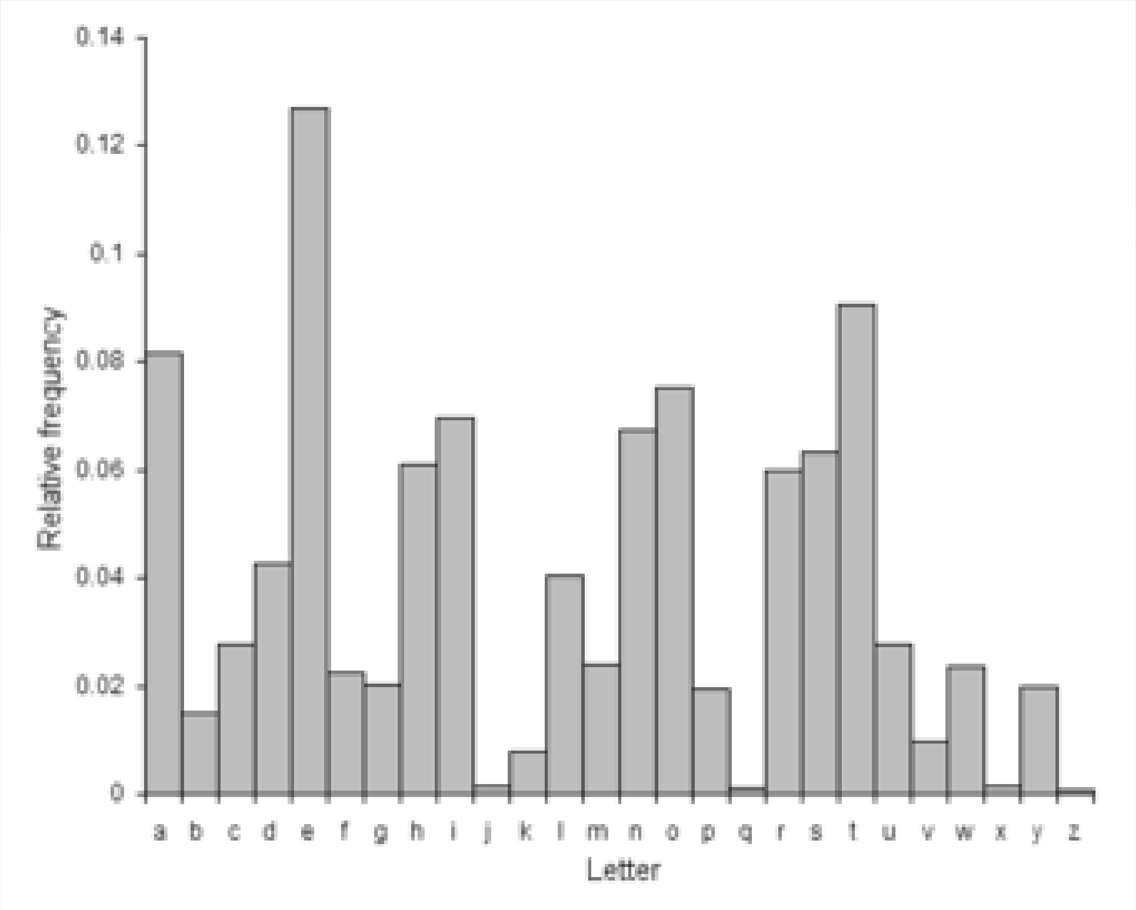
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Cryptanalysis of Substitution Ciphers

THIS IS A TEST => WKLV LV D WHVW

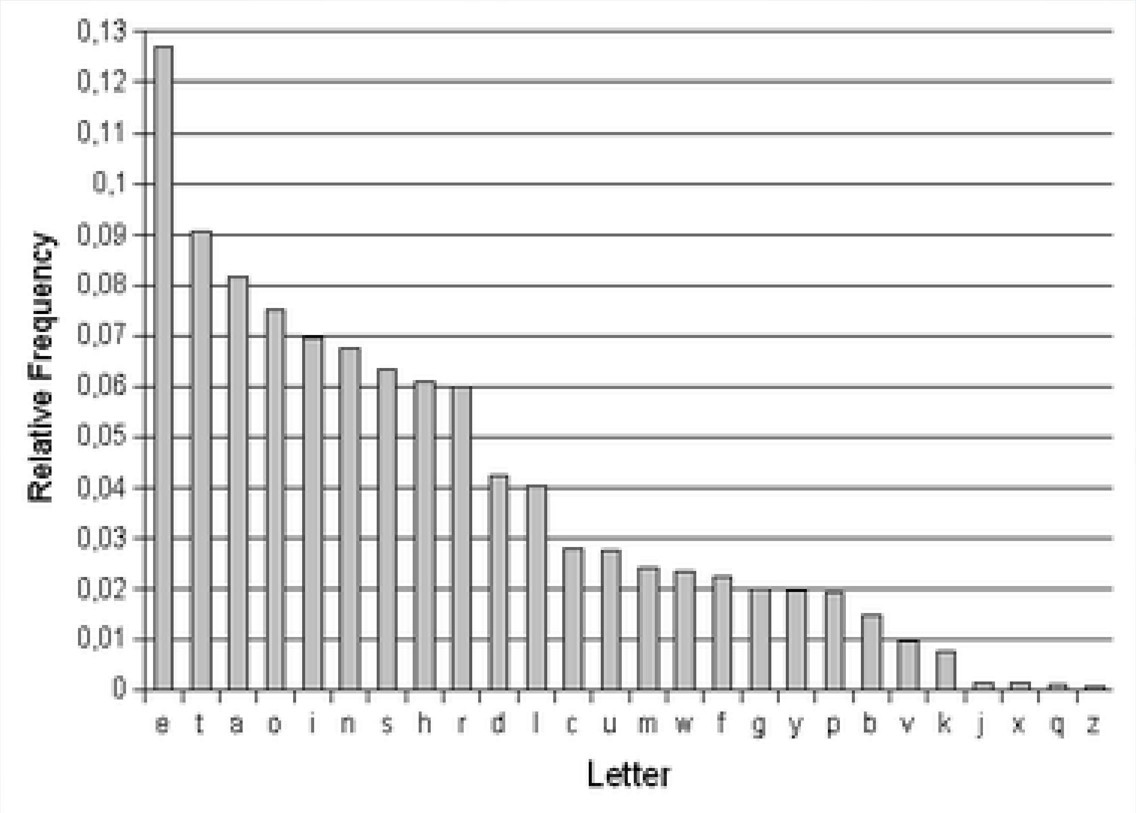
- Spaces in ciphertext give sentence structure
- Substitute small words in ciphertext
- Guess repeated characters
- Apply logic to the rest of the message
- Easy to break based on rules of English

Letter frequencies in English text



Source: Wikipedia

Letter frequencies in English text



Source: Wikipedia

Cryptographic Techniques
Polyalphabetic – Vigenere Cipher

YOU ARE GOOD

K1=4,K2=2

YOU ARE GOOD

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Cryptographic Techniques
Concealment

- Introduces additional symbols in the ciphertext to conceal the content
- E.g. example below introduces a random character after every valid character

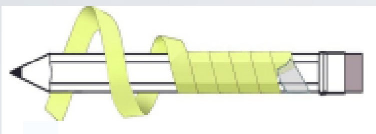
Plaintext	C		O		D		E		D
Ciphertext	F		R		G		H		G
Concealment	F	X	R	C	G	D	H	Z	G

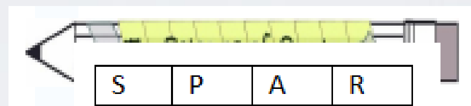
- Can give considerable security, but can greatly expand the message

Scatyle cipher – what is the underlying cryptographic technique?

menti

- Encrypt (by sender Alice)





S	P	A	R
T	A	U	N
D	E	R	A
T	T	A	C

Plaintext

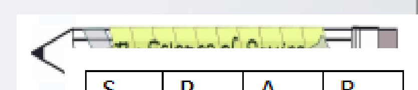
Encrypt

Ciphertext

S T D T P A E T A U R A R N A C

- Decrypt (by recipient Bob)

Decrypt



S	P	A	R
T	A	U	N
D	E	R	A
T	T	A	C

Cryptographic Techniques
Product Ciphers

- Combine two or more of the basic methods
- Claude Shannon showed that alternating approaches can produce strong ciphers from weak components
  - provides the basis for more complex algorithms to be introduced later
- A very simple example, using just one instance of substitution, followed by one instance of transposition is as follows . . .

Product Cipher: Example

Substitution (using Caeser)

T	H	I	S		I	S		E	N	C	R	Y	P	T	E	D
W	K	L	V		L	V		H	Q	F	U	B	S	W	H	G

Transposition

W	K	L	V
L	V	H	Q
F	U	B	S
W	H	G	

Ciphertext

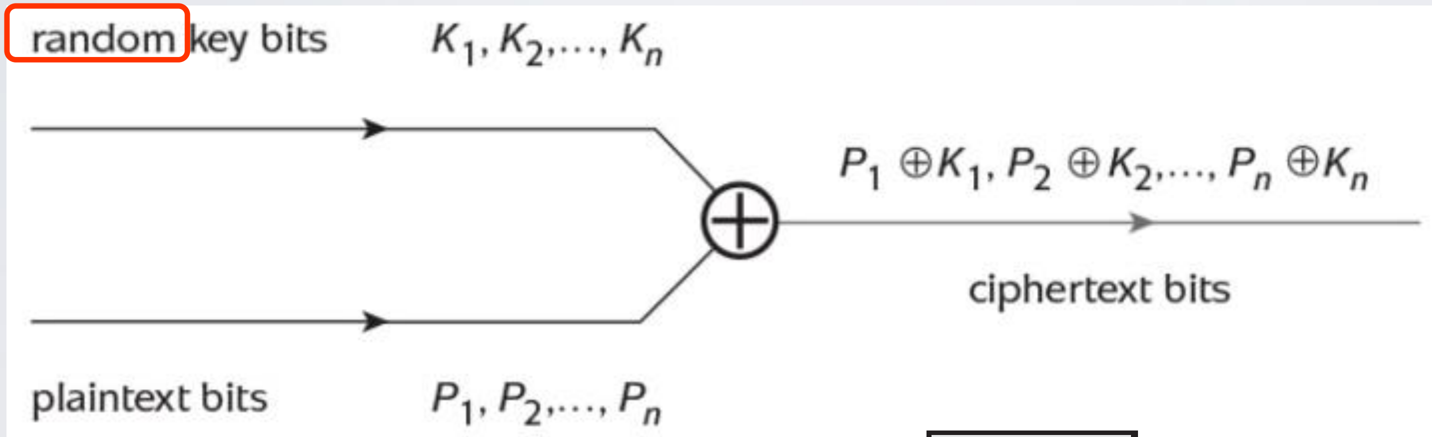
WLFW KVUH LHBG VQS

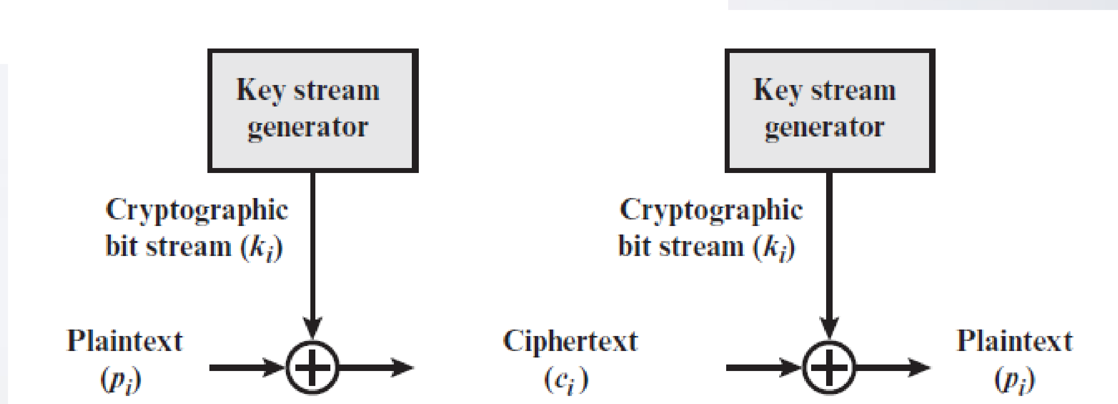
One-Time Pad

- A one-time pad is a key sequence at least as long as plaintext
- Each side of the communication has an identical pad
- It is a perfect cipher system, in the sense that no matter how much computational power you throw at the ciphertext, you cannot break the ciphertext
- However, it is difficult to use in applications which consume a large amount of key material
- OTPs also provide only confidentiality, not data integrity

Vernam Cipher or One-time pad

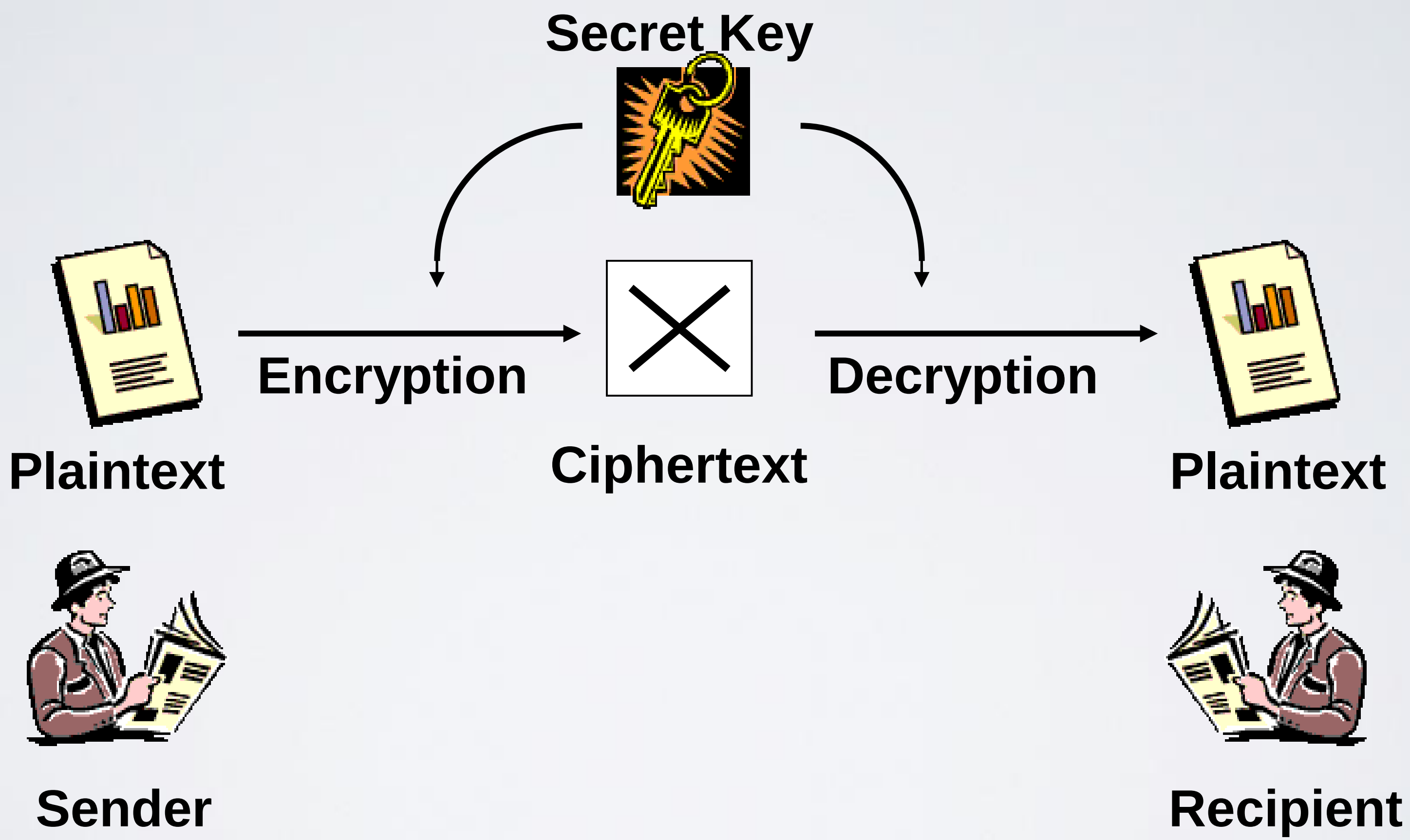
- By Gilbert Vernam in 1918 at AT&T.
- Against cryptanalysis of polyalphabetic ciphers
- Key length = message length
- No statistical relationship between key and plaintext.





- Resume at 12.00
- Check in: BD JQ UZ

Symmetric Algorithm



What symmetric encryption is being used?

- iCloud: 128-bit AES
- Facetime, iMessage: 256-bit AES in CTR mode
- Whatsapp: 256-bit AES in CBC mode
- Adobe Reader: supports 256-bit AES
- SSL/TLS: allows to use AES

https://support.apple.com/en-us/HT202303

Asymmetric Cryptography

- AKA Public Key Cryptography

- Solves the key distribution problem :
  - based on a pair of keys per user
  - messages for user are encrypted using freely available **public key**
  - can only be decrypted using **private key** - known only to the user and never shared
  - knowledge of the public key does not give any clue to the private key

Public Key Cryptography

- Originally due to Diffie and Hellman (1976), and independently discovered by Ellis at GCHQ (1970)

- Secret key cryptography shares a secret, the key. This must be distributed somehow prior to any secured communications

- The essence of public key cryptography is that two related keys are used:
  - *Alice produces two keys, the public key K_A, and the secret key K_A^{-1}. Although Alice can easily generate this keypair, it should be difficult for Charlie, who only has K_A, to compute K_A^{-1}.*

Public Key Cryptography

- With this property in mind, Alice can publish the key with the legend “This is Alice’s public key”

- Bob can then create a message *M,* which he encrypts using Alice’s public key:

$$C=E_{KA}(M)$$

- Alice, as the sole possessor of K_A^{-1} computes:

$$M=D_{KA\text{-}1}(C)$$

- However, Charlie can publish K_x and mark it as ‘this is Alice’s public key’. Then when Bob creates:

$$C=E_{Kx}(M)$$

- Only Charlie (who holds K_X^{-1}) can decrypt it

Public Key Generation

- Public key systems commonly based on one of 3 types of mathematical problem computationally difficult):
  - Integer Factorisation Problem (e.g. RSA)
  - Discrete Logarithm Problem (e.g. DSA)
  - Elliptic Curve Discrete Logarithm Problem
- None of the underlying mathematical problems have been proven to be intractable
- However, they are believed to be intractable :
  - years of intensive study have failed to yield efficient algorithms to solve them.

Encrypt/ decrypt (confidentiality)

- Senders: students, recipient: lecturer
- Lecturer publishes public information: N=33, public key e=3
- Go to

https://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo/bob.html

- Choose “Encryption Page”
- Encrypt using RSA with

“Pick a letter to cipher” means your plaintext

“Enter Alice’ exponent key, E” means the recipient’s public key e=3

“Enter Alice N’s value” means the public information N=33

Choose Encrypt

Write your ciphertext to Menti

Message authentication (integrity)

- Sender: lecturer, recipients: students
- Lecturer sends the combined information: (plaintext=B, encrypted message=32,N=65, public key=29)
- Go to

https://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo/bob.html

- Choose “Decryption Page”
- Decrypt using RSA with

“Enter the encrypted message”: 32

“Enter your N value”: 65

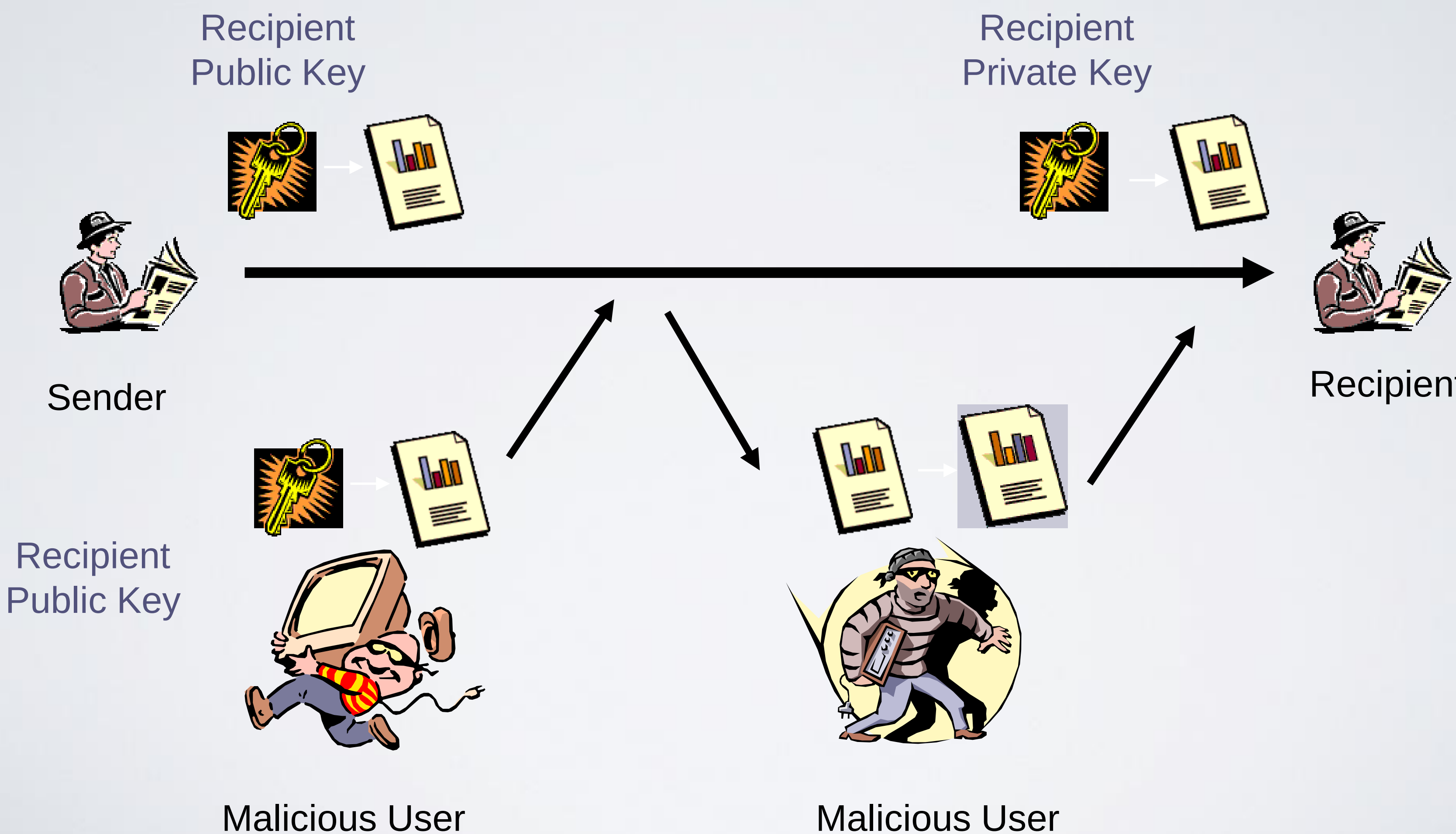
“Enter your private key”: 29

Choose Proceed

Is the decrypted message similar to the received plaintext (B)?

Write your plaintext to Menti

Message Integrity & Authentication



One Way Hash Function

- To ensure integrity a mechanism is required that can create a “fingerprint” of the data

- Hash functions allow us to take a variable length input and produce a fixed length output that “uniquely” fingerprints the input

- Key characteristics:
  - Given *M*, it is easy to compute *h*
  - Given *h*, it is hard to compute *M* such that *H(M) = h*
  - Given *M*, it is hard to find another message *M’*, such that *H(M)=H(M’)*

One-Way Property

Strong Collision Resistance

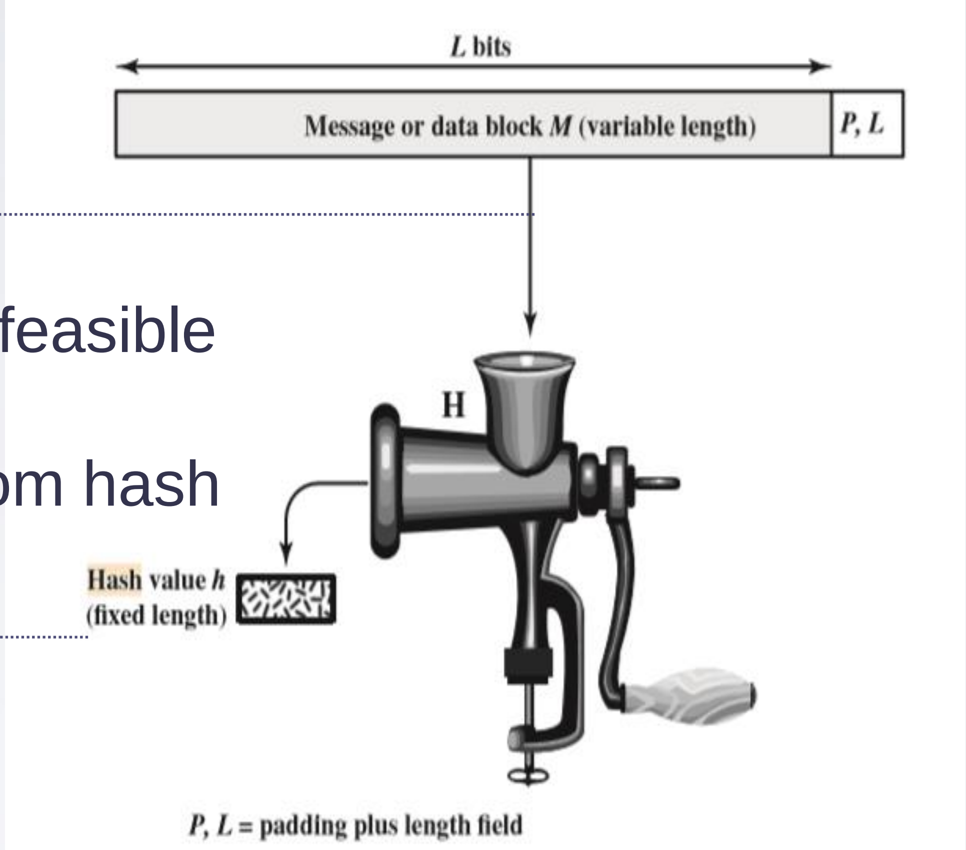
One Way Hash Function

Input message:
any size

Easy to
compute

One way: infeasible
to find input
message from hash
value

Hash value:
fixed size



A hash function accepts a variable-size message *M* as input and produces a fixed-size output, referred to as a **hash value/ hash code** H(*M*)

Calculate hash

- Choose a message
- Calculate hash value using https://academo.org/demos/SHA-256-hash-generator/
- Change only 1 letter of your message
- Re-calculate hash value using https://academo.org/demos/SHA-256-hash-generator/
- Compare it with the previous hash value

Birthday Attack

- Two Brute Force attacks against one-way hash functions:
  - An adversary wants to find two random messages , M and M’ such that H(M)=H(M’)
  - Finding two messages that hash to the same value requires $2^{m/2}$ random messages
  - A 64-bit hash would take a machine capable of 1 million hashes per second could find a pair of messages in about an hour
- This is known as a Birthday attack.

- It is significantly different to the second attack:
  - Given the hash of a message, H(M), an adversary creates another message, M’ such that H(M)=H(M’)
  - This is a much more difficult task to achieve – finding a message, *m* that hashes to a given hash requires hashing 2^{m} random messages
  - A 64-bit hash would take a machine capable of 1 million hashes per second 600,000 years to find a second message

Message Authentication Codes

- MAC – a key dependent one-way hash function
  - Exactly the same operation as one-way hash functions except only someone with the key is able to verify the hash.
  - Provides *authenticity* of the message
  - Does not provide confidentiality
- A person could use a MAC to ensure his files have not been altered.
- Simple MAC – use a one-way hash function with a symmetric key
- Any MAC can be made into a one-way hash function by simply making the key public

Message authentication (integrity)

- Sender: lecturer, recipients: students
- Lecturer sends the combined information: (plaintext=“class at 11am”, secret key=pass, hash code= 61f44a70b686df32b7daa62346d661062fb118a6b8ea866a61049a30d 8d74f36)
- Go to

https://academo.org/demos/SHA-256-hash-generator/

Calculate hash code of the combined message of plaintext and secret key (class at 11ampass)

Is the hash code similar to the received one?

- Message: asdfmovieisgreat
- Received Hash code: 2a43fd82a10c447e171bf266f43c1be95e0c8ecb14d670ed19fd8dfc49ac6df7
- MITM

asdfmovieisgreat -> modify to asdfmovieisnotgreat

Does not know key

Received hash code:

76a2fa0af8d111dd0c66ea1d4addb24f35e16b6766caa2b1cc580182009aa8f9

E

Calculated hash code:
f43b237c30ac2c6024cc9663e2d9ea632b4cd3cd5ea5b6c27ac7e630381e3f36

Fake MAC

- Get the message of the volunteering group
- Calculate a hash value
- Compare it with the true hash value

Digital Signature

- If E and D are left and right inverses of each other, we can use them for message authenticity as well as confidentiality

- Alice can take her message and subject it to decryption: (encrypt using private key)

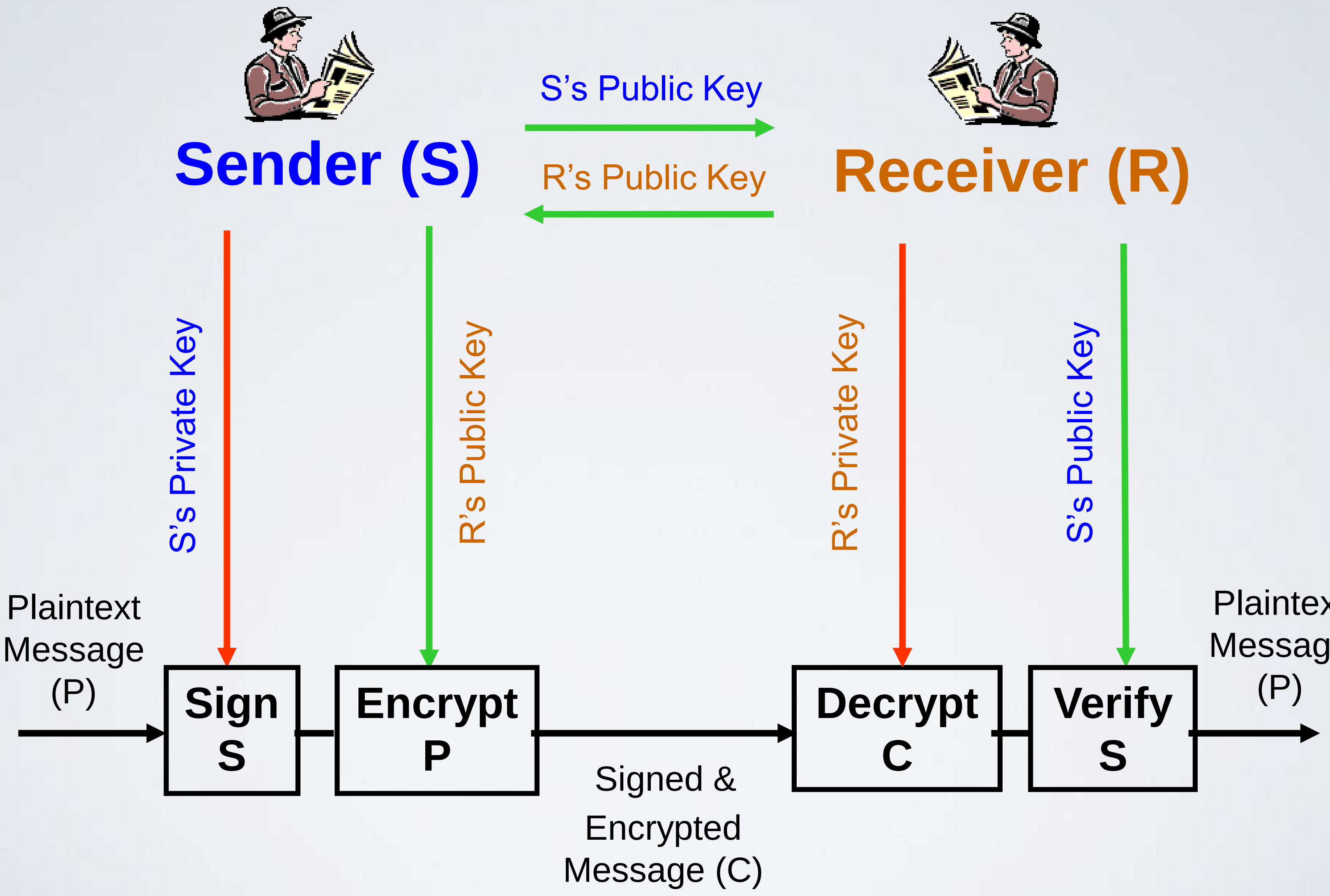
$$S=D_{KA\text{-}1}(M)$$

- Anyone with K_A can use it to recover M (decrypt using public key)

$$M=E_{KA}(S)$$

- This decryption S is usually called a digital signature

Encryption and Signature



Sign the document

Alice

- Message: E
- Private key: 43
- Public: 85
- Sign(E) = Encrypt_RSA(E, key = 43) = 83 (signature)

Alice sends (E,83) to Bob

Bob: verify the signature

Verify(83): Decrypt_RSA(83, key=3)=E

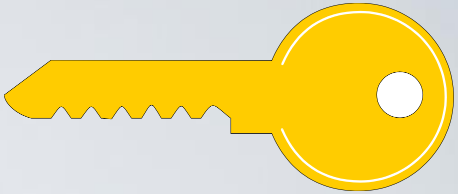
Verify signature

- Menti
- Receive the public key
- Receive the message and its signature
- Verify the message by using RSA decryption with the provided key

Fake signature

- Given the message
- Can you fake the signature?

Using keys



Required action	Whose key	Key type
Send an encrypted message	Receiver's	Public
Sign a message	Sender's	Private
Decrypt an encrypted message	Receiver's	Private
Authenticate a signed message	Sender's	Public

Key Distribution

Key Management

- Where are keys generated?
- How are keys generated?
- Where are keys stored?
- How do they get there?
- Where are the keys actually used?
- How are keys revoked and replaced?

- Protect keys:
  - Systems security, access control mechanisms

- Cryptography is a translation mechanism, converting a communications security problem into a key management problem…and ultimately into a computer security problem

Cryptanalysis

Cryptanalysis

- Cryptanalysis is the science of recovering the plaintext of a message without access to the key
  - Although successful cryptanalysis may recover the key

- Fundamental assumption in cryptanalysis:
  - Secrecy must reside in the key *not* the algorithm
  - The cryptanalyst has complete details of the cryptographic algorithm

  - In a real-world situation it is unlikely that the cryptanalyst has so much information
    - However, if the cryptanalyst is unable to break the algorithm *with* knowledge of the system, they certainly are not going to be able to break the system *without* the knowledge

Cryptanalysis

- menti

1. Ciphertext: UUNAQMT
2. Cryptanalyse using Brute force attack
   https://www.dcode.fr/transposition-cipher
3. Write the plaintext to menti

Conclusions

Conclusions

- Cryptography enables you to construct a secure logical channel over an insecure physical connection
- Currently most attackers will seek to attack vulnerabilities other than cryptanalysis
- Cryptography is *not* the holy grail of security
- Only through careful systems planning can encryption operate effectively
- Systems security has an integral role to play in security provisioning

UNIVERSITY OF PLYMOUTH

Dr Hai-Van Dang

hai-van.dang@plymouth.ac.uk

Centre for Security, Communications & Network Research

www.plymouth.ac.uk/cscan