School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko

Cybersecurity Fundamentals

Classical Cryptography I

Learning objectives

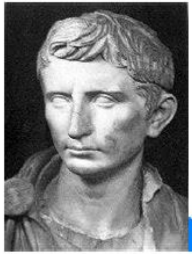
- Define key terms such as **cipher**, **cryptography**, **cryptanalysis**, **plaintext**, **ciphertext**, **keys** and the role of Alice, Eve and Bob.
- Describe and compare the security of three classical symmetric algorithms (ciphers) for transforming plaintext in ciphertext: **substitution**, **polyalphabetic substitution** and **one-time pad**.
- Classical cryptosystems (substitution, transposition, and polyalphabetic substitution)

PART I:
Cryptography history and terminologies

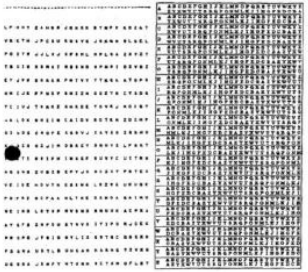
Cryptography

- **kryptós** “hidden, secret” and **graphein**, “to write”
- Specialised area of mathematics
- Protect information (**confidentiality**, **integrity**)
- Against an adversary who wishes to **intercept** or **modify** the data.
- Lack of use of cryptography resulted in many data breaches
- Used on the web, accessing remote systems, fundamental to financial systems

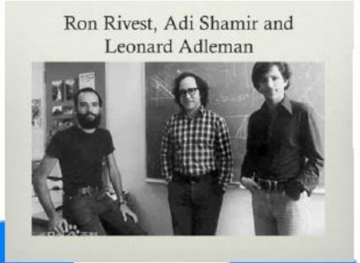
State-of-the-art over the ages



Caesar
(100 BC-44 BC)

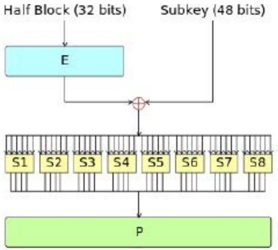


Frank Miller
(1842-1925)

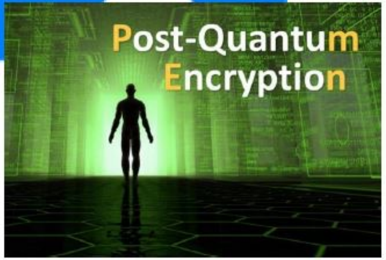


RSA (1977)
also GCHQ

Vigenère
(1523-1596 CE)



IBM (DES)
(early 1970s)



????

Some key terms

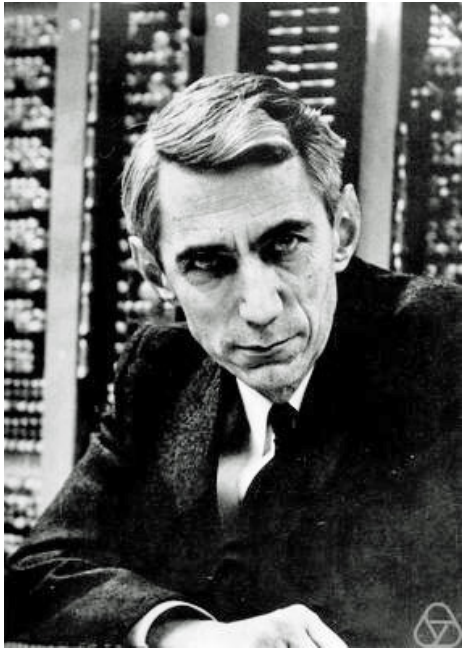
- **Plaintext** - directly read by humans (used to be text, now its bits and bytes)
- **Ciphertext** – encrypted data
- **A cipher (or cryptographic algorithm)** – mathematics or algorithm that turns ciphertext into plaintext (and vice a versa)
- **Encryption** – the process of “encipherment”
- **Decryption** – the process of “decipherment”

Types of cryptography technologies

- The type of operations used for transforming plaintext to ciphertext
  - *Substitution, transposition, product systems*
- The number of keys used
  - One key or different keys
- The way in which plaintext is processed
  - Block cipher, stream cipher

Encryption keys

- **Keys** determine the output from encryption and decryption process
- Key must be kept secret **but not the cipher algorithm**.
- Claude Shannon "one ought to design systems under the assumption that the **enemy** will immediately gain **full familiarity** with them"
- Keys in the following examples are characters, but a computer encryption key is a string of bits (01010111….)
- The total number of keys is $2^{\text{key length}}$



Problem with short keys

- Besides frequency analysis and other methods, can try to brute force it!
- **Brute force = try all combinations**
- How long should a key be?
- It depends upon the power of the attacker.
- GPUs can test 100s of millions of symmetric cryptographic systems per second

What should we look for?

- An encryption scheme is computationally secure if the ciphertext generated by the scheme meets one or both of the following criteria:

    The cost of breaking the ciphertext exceeds the value of the encrypted information

    The time required to break the ciphertext exceeds the useful lifetime of the information

Quick exercise

- A 128-bit secret key is used. 1 second is needed to check one candidate key. How long will it take, on average, to find the secret key and decrypt the message?

Quick exercise

- A 128-bit secret key is used. 1 microsecond is needed to check one candidate key. How long will it take, on **average,** to find the secret key and decrypt the message?

PART II:
Mathematical foundations

Modular arithmetic

- Divide two integers

$$\frac{A}{B} = Q \text{ remainder } R$$

  - A is the *dividend*
  - B is the *divisor*
  - Q is the *quotient*
  - R is the *remainder*

- 11 divided by 5
  - A = 11, B = 5
  - 11 divided by 5 = 2
  - Remainder is 11 - 2 * 5 = 11 – 10 = 1

Modular arithmetic

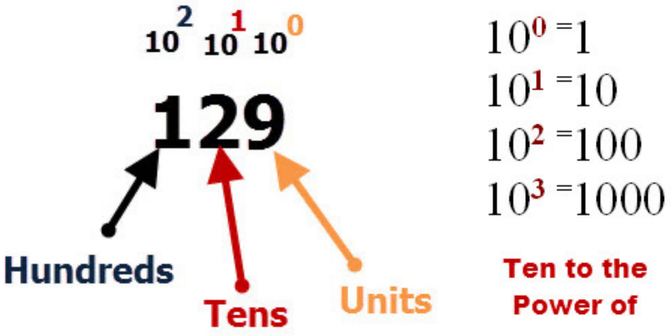
- Sometimes, we are only interested in what the **remainder** is when we divide A by B.
- For these cases, there is an operator called the ***modulo*** operator (abbreviated as **mod**).
- Using the same A B, Q and R as above, we would have: A mod B = R
- We would say this as A modulo B is equal to R. Where B is referred to as the modulus.
- 11 mod 5 = 1 because 1 is the remainder of 11/5
- 3 mod 5
  - 3 divided by 5 = 0
  - Remainder is 3 – 0 x 5 = 3 - 0 = 3
- 15 mod 5
  - 15 divided by 5 = 3
  - Remainder is 15 – (3 x 5) = 15 = 0

Introducing binary and hexadecimal

- Decimal numbers are the countable numbers we use on an everyday basis and use base 10, e.g. 1, 2, 3, ... 20, 21, …
- Binary numbers are used internally by computers and are numbers expressed using base 2, e.g. 1, 01, 11, …, 10100, 10101, …
- Hexadecimal numbers are often used by programmers because easy to convert to binary but take up less space when written, e.g. 1, 2, 3, …, 14, 15 …

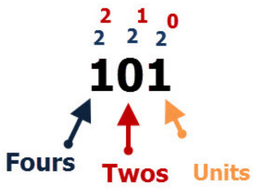
Overview of decimal numbers

- Our decimal system uses 10 as a base
- Numbers range from 0 to 9
- Example 129
  - 100 + 20 + 9 = 129
- We can express this in terms of powers of base 10 as well



Binary number system

- Binary numbers are base 2 numbers, and have only two values – 0 and 1.
- If we look at a binary number like 101, then we can again assign column values as we did with our decimal number, but this time we use 2, and not 10 as the base.
- So binary 101 binary has 1 in the units column,0 in the 2s column and 1 in the 4s column.
- Again if we work our way from right to left then:
- The 1 is a 1 as it is in the units column but the next 1 is not 1 but 1*4=4



$2^0 = 1$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

Hexadecimal number system

- Hexadecimal numbers are base 16 numbers.

Binary	Hex
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Examples

- This is a useful tool: https://www.rapidtables.com/convert/number/binary-to-decimal.html

- And a good reading: https://www.csfieldguide.org.nz/en/chapters/data-representation/numbers/

PART III:
Classical cryptography

Classical cryptosystems

- Transposition
  - Columnar
  - Scytale
- Substitution
  - Caesar
- Polyalphabetic substitution
  - Viginere
  - One time pad

These are all symmetric cryptosystems

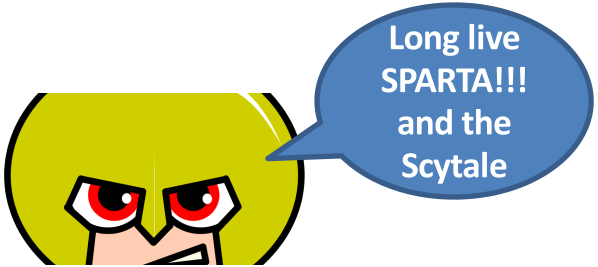
Concept: *Transposition* ciphers

- Break a plaintext up into characters.
- Change the order of the characters according to fixed rules.
- Encryption algorithm:
  - Each character of the plaintext is reordered to form the ciphertext
- Decryption algorithm:
  - Each character of the ciphertext is reordered to form the plaintext

Example: Transposition ciphers

- Example is ***columnar*** transposition cipher
- Each plaintext character is written horizontally into a table with a specified alphabet.
- The table is read vertically in column order to create the ciphertext.
  - Plaintext **helloworld**
  - Ciphertext **holewdlo_lr**

h	e	l	l
o	w	o	r
l	d		



Concept: *Substitution* ciphers

- Break a plaintext up into characters.
- Replace characters according to fixed rules.
- Encryption algorithm:
  - Every occurrence of one character *substituted* with same replacement character to create the ciphertext

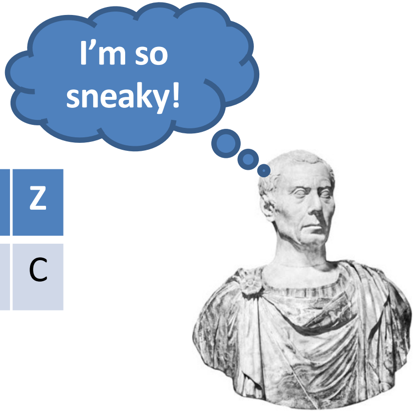
- Decryption algorithm:
  - *Substitute* each character of the ciphertext with the one that it originally replaced

Example: Caesar cipher

- Caesar (100-44 BCE) used to *encrypt* his messages using a very simple algorithm, which could be easily *decrypted* if you know the key.
- He would take each letter of the alphabet and replace it with a letter a certain distance away from that letter. When he got to the end, he would wrap back around to the beginning.
- Example with a shift of 3:

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
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

CAT becomes *FDW*



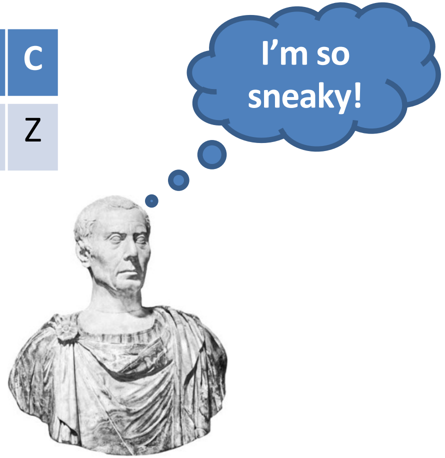
Example: Caesar cipher (cont.)

- Decryption requires applying the inverse of the shift operation, this could be represented as another table with the rows swapped.

- Example with a shift of 3:

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
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

FDW becomes *CAT*



Example: Caesar cipher

- You can use the shift value as the key for the cipher algorithm.

Shift = 3

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
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

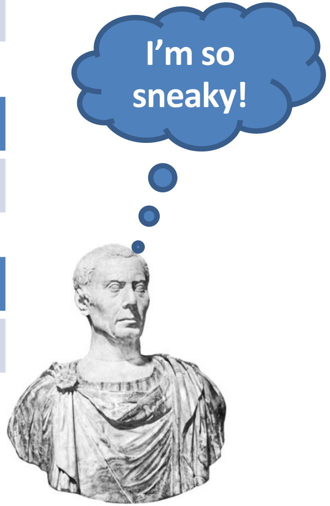
Shift = 4

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
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

Shift = 5

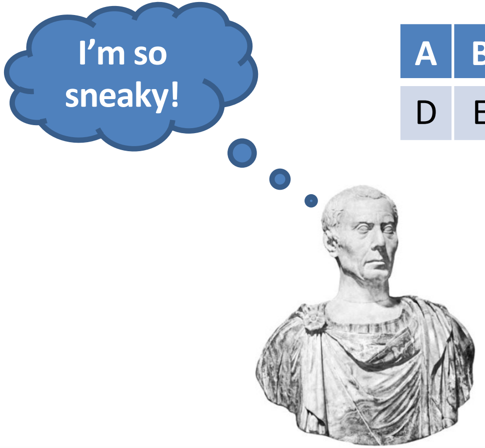
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

…



Question: how many keys?

- How many possible keys if the Caesar cipher is operating on the letters of the English alphabet A-Z?
- Is 0 a good choice of key?
- What about 26?



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
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

But I Don't Want to Make a Table!

- That's fine! If you know what the shift is, you can use something called ***modulo***, which is commonly shortened to **mod**.
- Let's say we wanted to find 8 mod 5. We would divide 8 by 5 and find the remainder. So, in this case, 8 mod 5 = 3.
- In this case, 5 is called the ***modulus***.
- Examples:
  - 19 mod 5 = ?
  - 2 mod 5 = ?
  - 25 mod 5 = ?

This week

- Labs start THIS week.

- On Tuesday,
  - we will continue with symmetric ciphers and related issues, and
  - discuss some modern symmetric cryptosystems.