Encryption

- A means of secretly communicating private messages via public channels
- Essential for the modern economy, the Internet, and the Web.

Caveat

- Cryptography is an arms race
- Material presented is obsolete, it illustrates the key principles

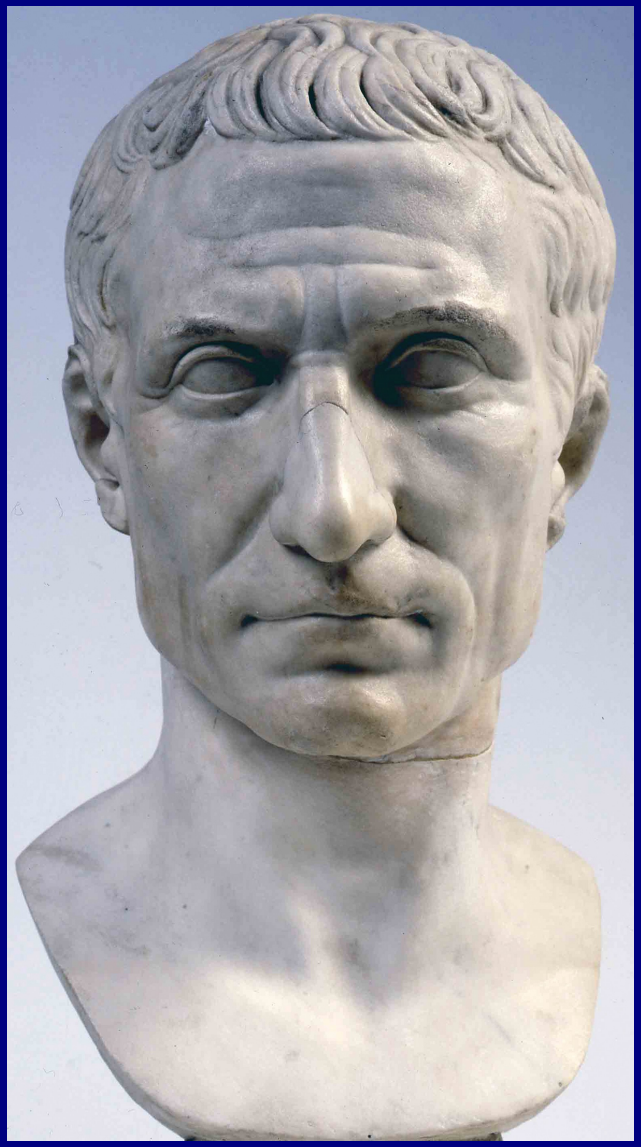
Terminology

- Plaintext - the original message
- Ciphertext - the encrypted version of the message
- Key - necessary information to convert between plaintext and ciphertext

Lexicographical Ordering

Letter	Number
A	1
B	2
C	3
D	4
E	5
...	
W	23
X	24
Y	25
Z	26

Caesar Cipher



Substitution Cipher

Letter	Number	Number + 3	Cipher Letter
A	1	4	D
B	2	5	E
C	3	6	F
D	4	7	G
E	5	8	H
...			
W	23	26	Z
X	24	1	A
Y	25	2	B
Z	26	3	C

"Send me a hundred more soldiers" becomes

"Vhqg ph d kxqguhg pruh vroglhuv"

Problems with Caesar Ciphers

- The "key" is the offset
- Only 25 offsets to try

Better Substitution Cipher

Letter	Cipher Letter
A	X
B	Q
C	K
D	R
E	A
...	
W	Y
X	B
Y	L
Z	T

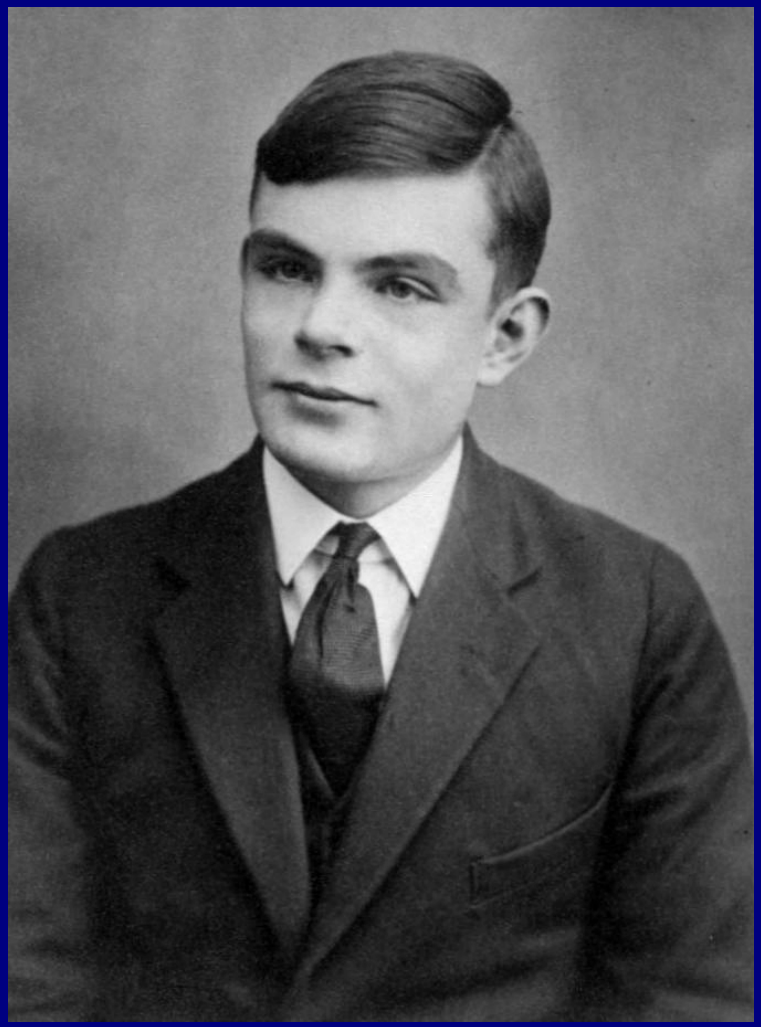
Problems

- The "key" is the mapping
- Statistical Attack: some letter occur more frequently
  e.g. r s t l n e
- Sender and Receiver must agree upon the key

The Enigma Machine

Enigma Problems

- Symmetric-key cryptography: Sender and receiver must share the key beforehand



One-Time Pads

One-Time Pads: substitution cipher for binary

$$0 \text{ XOR } 1 = 1$$
$$0 \text{ XOR } 0 = 0$$
$$1 \text{ XOR } 0 = 1$$
$$1 \text{ XOR } 1 = 0$$

Example

Plain text:	0 0 1 0 1 1 0 1
Key:	1 0 1 1 0 1 1 0 XOR
Cipher Text:	1 0 0 1 1 0 1 1

Why is it one-time?

key k, plaintexts t_1 & t_2:

$$(t_1 \text{ XOR } k) \text{ XOR } (t_2 \text{ XOR } k) = t_1 \text{ XOR } t_2$$

t_1 XOR t_2 reveals the bits in common.

One Time Pad Benefits & Drawbacks

- Almost unbreakable
- Key in the same length as the data
- The key must be exchanged beforehand
- Can be used offline, make two paper copies of the keys. Simple, low-tech, strong encryption

Block Ciphers

Goal: Break t into $t_1, t_2, \cdots t_n$ blocks and encrypt into $c_1, c_2, \cdots c_n$

Given $E(t_i)$ that encrypts t_i into c_i

Chaining: $E(t_{i+1}$ XOR $c_i) = c_{i+1}$

Block Chains?

Public Key Cryptography

- Public Key: F_p, know to everyone and used to encrypt messages
- Secret Key: F_s, know only the receiver, used to decrypt messages
- $t = F_s(F_p(t))$
- Anyone can send a message, only the receive can decrypt

Public Key Cryptography

Digital Signing

- Digitial signing - encrypting with the secret key
- $t = F_p(F_s(t))$
- Any can receive the message, only the sender can encrypt

RSA Setup

- Public Key Crypto. Example: RSA
- Property 1: A factoring a number that is the product of two large primes is hard (NP)
- Property 2: Determining if a number is prime easy (P)

RSA

procedure RSA

Pick two large primes (1024 bits) p and q

$n = pq$

$r = (p-1)(q-1)$

Pick small odd integer e relatively prime r

Compute d as the multiplicative inverse of e i.e $ed \ \% \ r = 1$

public key is $P = (e, n)$

secret key is $S = (d, n)$

$F_p(x) = x^e \ \% \ n$

$F_s(x) = x^d \ \% \ n$

end procedure

Read More

- Blowfish
- Twofish
- AES