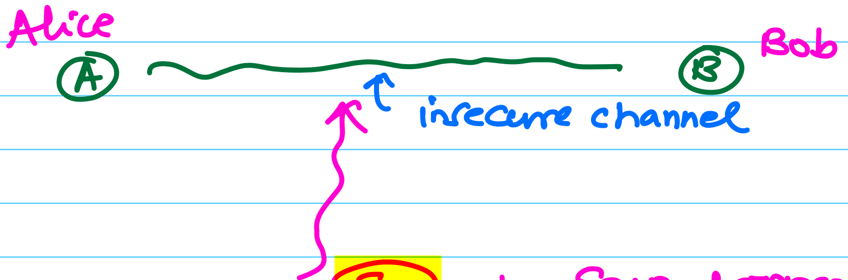
3rd Jan 2025

cryptography - crypto + graphos

Science of secret communication

where is it needed -

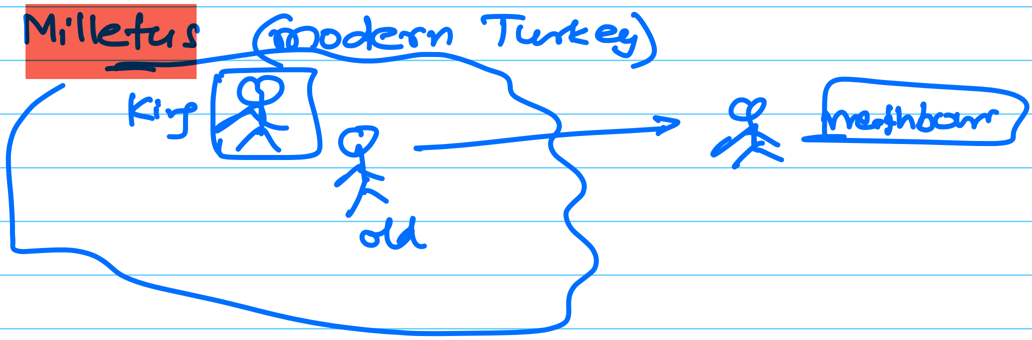
diplomatic missions,
soldiers, kings
lovers, e-commerce



Eve : Eavesdropper (passive)

Mallory : Malicious adversary (active)

Milletus (modern Turkey)



Slave — Shaved the head

Vietnam war   US army   Jeremiah Denton
captured by guirillas
BBC journalist — video interview

— — = 0   Morse code   • —
— —— = 1

Spelled "TORTURE"

YouTube video

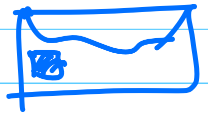
2nd war :

invisible ink

MI-2

o — Microdot

YouTube

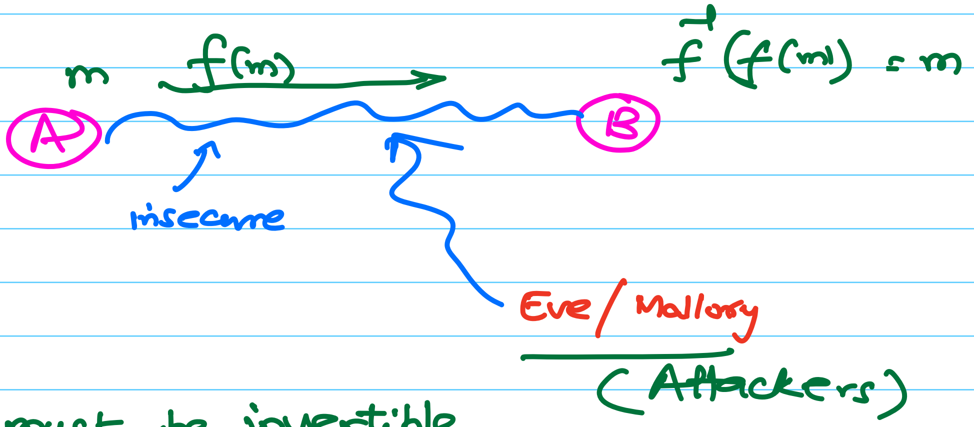


Steganography — "hide the method"

Cryptography — method is open

— yet secure communication

Setting.:



— method f must be invertible

— Alice knows f, Bob knows f^{-1}

But Attacker doesn't know f^{-1}.

Two way communication -

A, B : f, f^{-1}

attacker : doesn't have f^{-1}

Hiding the method

steganograph

CS: Algorithm Data → cryptography

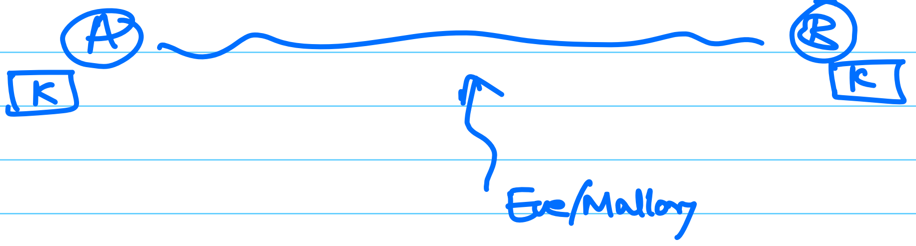
Without keeping "something" secret between A & B

— no secure communication is possible.

Secret data = secret key

(k)

$f(k,m) = c \longrightarrow f^{-1}(k,c) = m$



f: Encryption

f^{-1}: Decryption k = secret key

m = message/plaintext

c = ciphertext

Secret key
↓ ~~Encryption~~
Secret key cryptography

What is meant by "secret communication" ...

Historical examples.

Julius Caesar -

$$\begin{array}{cccccc} A, & B, & C, & \dots & & Z \\ \downarrow & \downarrow & \downarrow & & & \downarrow \\ 0 & 1 & 2 & & \dots & 25 \end{array}$$

$\mathbb{Z}$ = set of integers $\mathbb{Z}_{26} = \{0, 1, \dots 25\}$
op' modulo 26

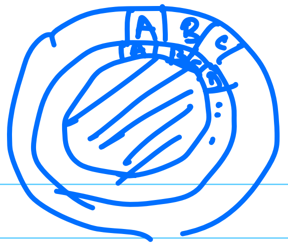
$x, y \in \mathbb{Z}_{26}$

$x + y = (x+y) \bmod 26$ remainder

key = k, msg = m, ciphertext = c

$Enc(k, m) = (m+k) \bmod 26$

$Dec(k, c) = (c-k) \bmod 26$



Encryption/ decryption is letter by letter

$$m, c \in \mathbb{Z}_{26}$$

$$k \in \mathbb{Z}_{2}$$

Shift cipher

$$Enc(k, m) = (m+k) \bmod 26$$

$$Dec(k, c) = (c-k) \bmod 26$$

ciphertext = PIIPRZ

plaintext = ?

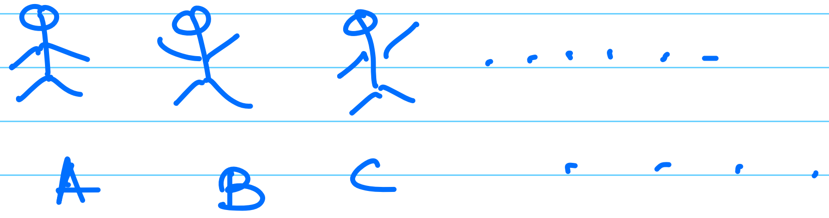
k	plausible plaintext
1	OHHOQY
2	. . .
3	. . .

complexity of bruteforce = $O(n)$

practically, you expect $\sim \frac{(n+1)}{2}$ ←

Sherlock Holmes : A. C. Doyle

"The adventure of the dancing men"



Secret key = mapping.

How many mappings?

$$= 26!$$

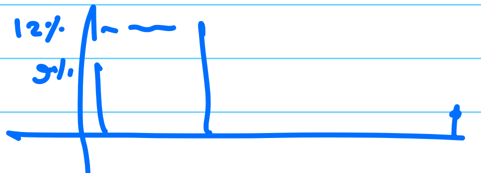
$$n! \sim n^{n+1/2}$$

plaintext ↓ ciphertext

$$26^{24} \text{ to } 26^{25}$$

$$\sim 2^{88}$$

Statistics are preserved



QU = double character

TH_

Define — secure encryption → Create such methods
more security goals