Cryptography

Lets learn about Encryption and Decryption

Julius Caesar

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the “shift by 3” rule could decipher his messages.

We must attack at dawn

Messenger! Pass this message onto my army at the frontline:

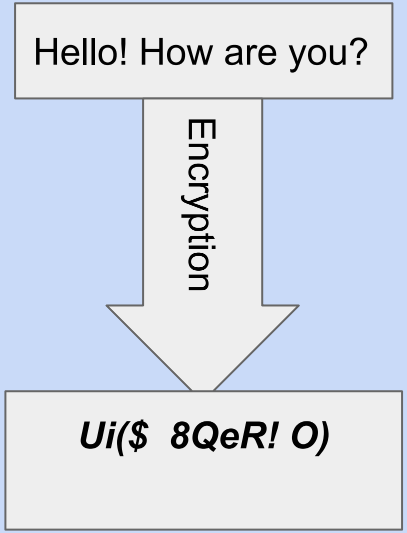
DWWDFN DW GDZQ !

2000 YEARS LATER, WE ARE STILL DOING SOMETHING VERY SIMILAR TO SEND MESSAGES SECURELY!

- Data that can be read and understood without any special measures is called **plaintext** or cleartext. Here's some plaintext*:* *"Hello! How are you?"*

- Sometimes, we want to no-one to know the information we are sending to someone else. It could be a very important instruction, a key combination to a safe or someone's bank account details. Here's the challenge then – how do we 'disguise' our information?

- The method of disguising plaintext is called **encryption**. Encrypting plaintext results in unreadable gibberish called **ciphertext**.

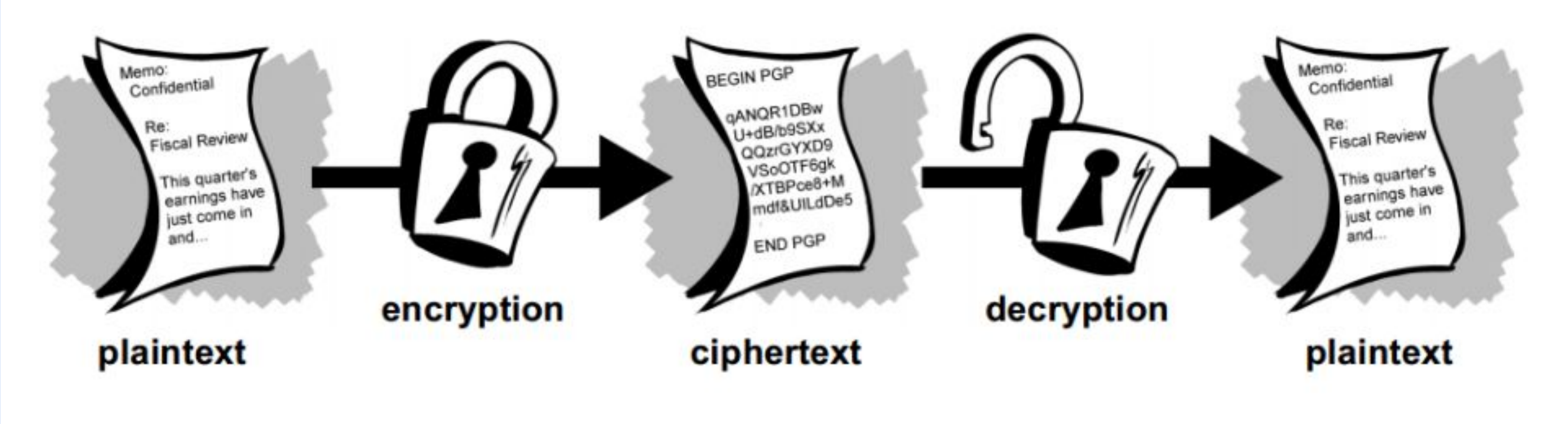


Hello! How are you?

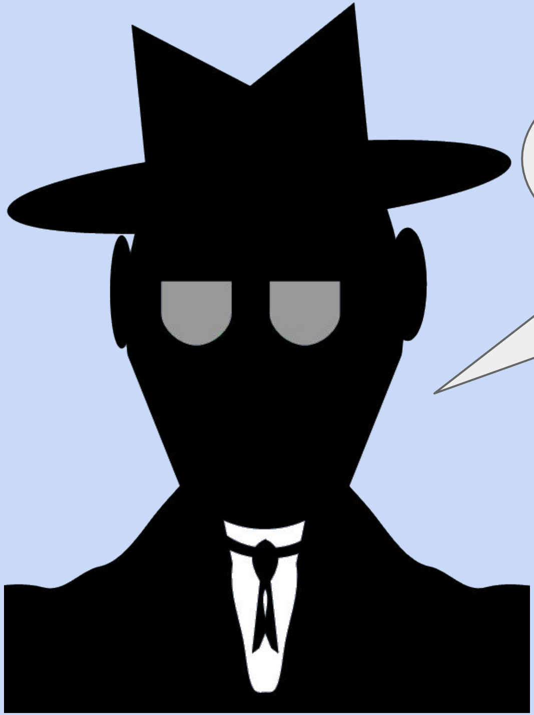
Encryption

Ui($ 8QeR! O)

Process of encryption and decryption



Simple ciphertext. Can you decode it?



(Encrypted SMS Text reads)

teeM em ta eht kcolc rewot ta 9.

Decoded message says . . . .

Let's find out if you decoded the message correctly

- It was disguised in a way which wasn't very complicated and all of the characters were already there.

- There are many ways of scrambling this plaintext to make it difficult to read. It can be done just by using some re-arrangement of the message without changing aNy of the actual letters.

Message: Meet me at the clock tower at 9

Different ways of scrambling the plaintext

Take the message: `Meet me at the clock tower at 9`

- By regrouping the letters but keeping them in the same order we can make it look nonsense:

  Meetme atthecl ocktow erat9

  Or

  Me etm ea tth ecl ock to wer at9

- Even without regrouping, if the whole message is written backwards it is not easily readable.

  9 ta rewot kcolc eht ta em teeM

- It is much worse if it is written backwards and re-grouped!

  9t are wot kco lce htt aemt eeM

  Or

  9 t ar e wot k co l ce ht t ae mt e eM

Task - Decode the messages

Try making sense of these. Each is a perfectly ordinary sentence in English which has been turned into apparent nonsense by using tricks explained the the previous slide.

1. THEC ATSA TONT HEMAT

Plain Text:

2. TOW INTH ERA CEYO UMU STR UNF AST

Plain Text:

3. WEN EED WAT ERA NDA IRS OAS TOL IVE

Plain Text:

Task continued….

1. ONAHO TDAYA COOLD RINKI SNICE

Plain Text:

2. LIAT OT DAEH MORF OG TAC A GNIKORTS NEHW

Plain Text:

3. TAM EHT NO TAS TAC EHT

Plain Text:

4. ECINS IKNIR DLOOC AYADT OHANO

Plain Text

1. SGOD DNA STAC EKIL ELPOEP TSOM

Plain Text:

2. EMOS SDRIB NAC YLF YREV HGIH

Plain Text:

3. RUO FEK AMO WTD NAO WT

Plain Text:

4. REEB SI EDAM MORF YELRAB DNA SPOH

Plain Text: