CS431

Computer and Network Security

# Cryptography

Abhishek Bichhawat

27/02/2024

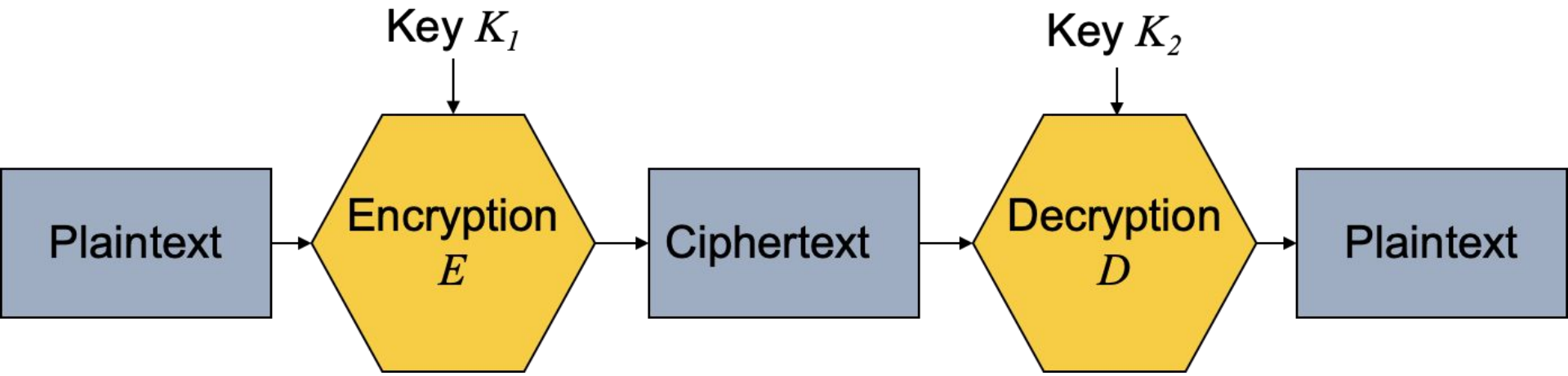
# Crypto...

- Cryptology is the study of Cryptography and Cryptanalysis
- Cryptography is the study of mathematical techniques to enforce security properties
  - Only (one of many) means to an end
- Cryptanalysis is the study of how to break cryptographic systems

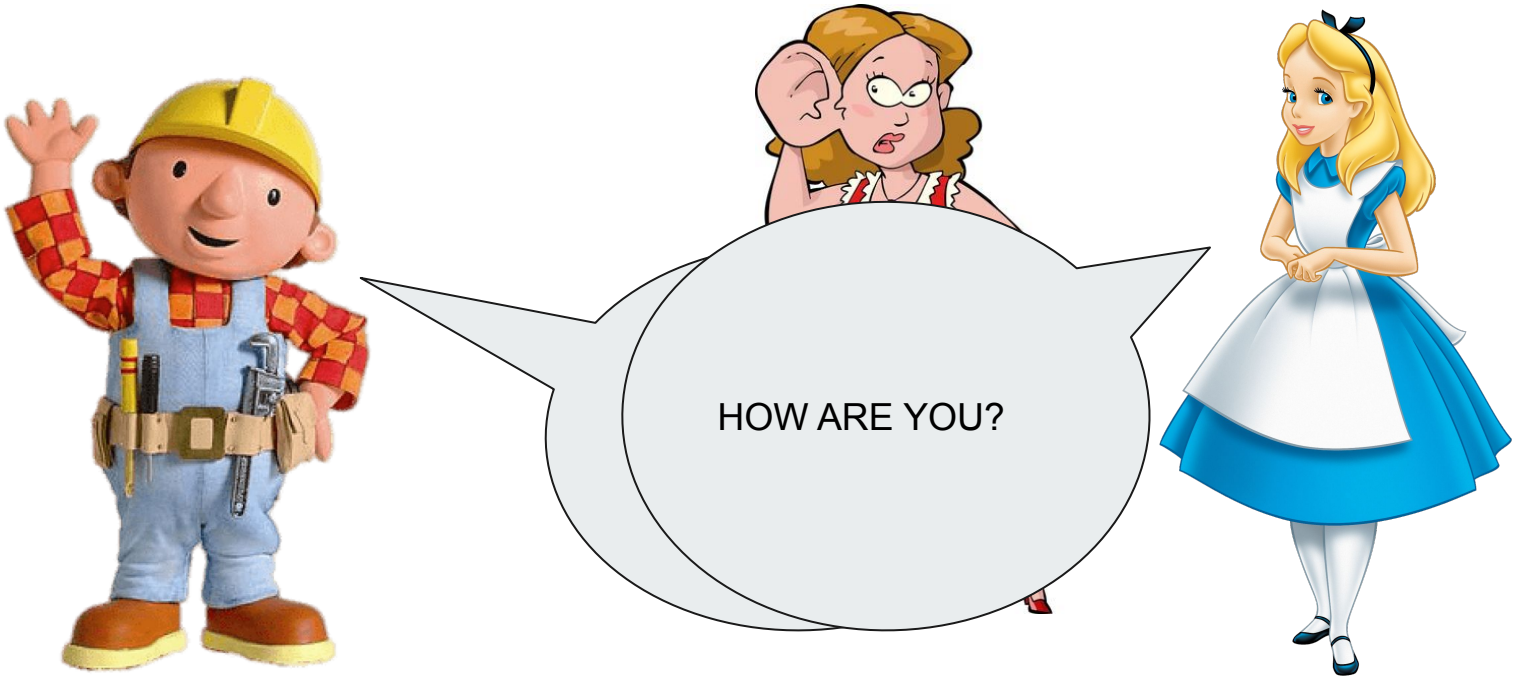
# Cryptography

- Idea of cryptography was to secretly transmit messages
- Secure communication between two parties

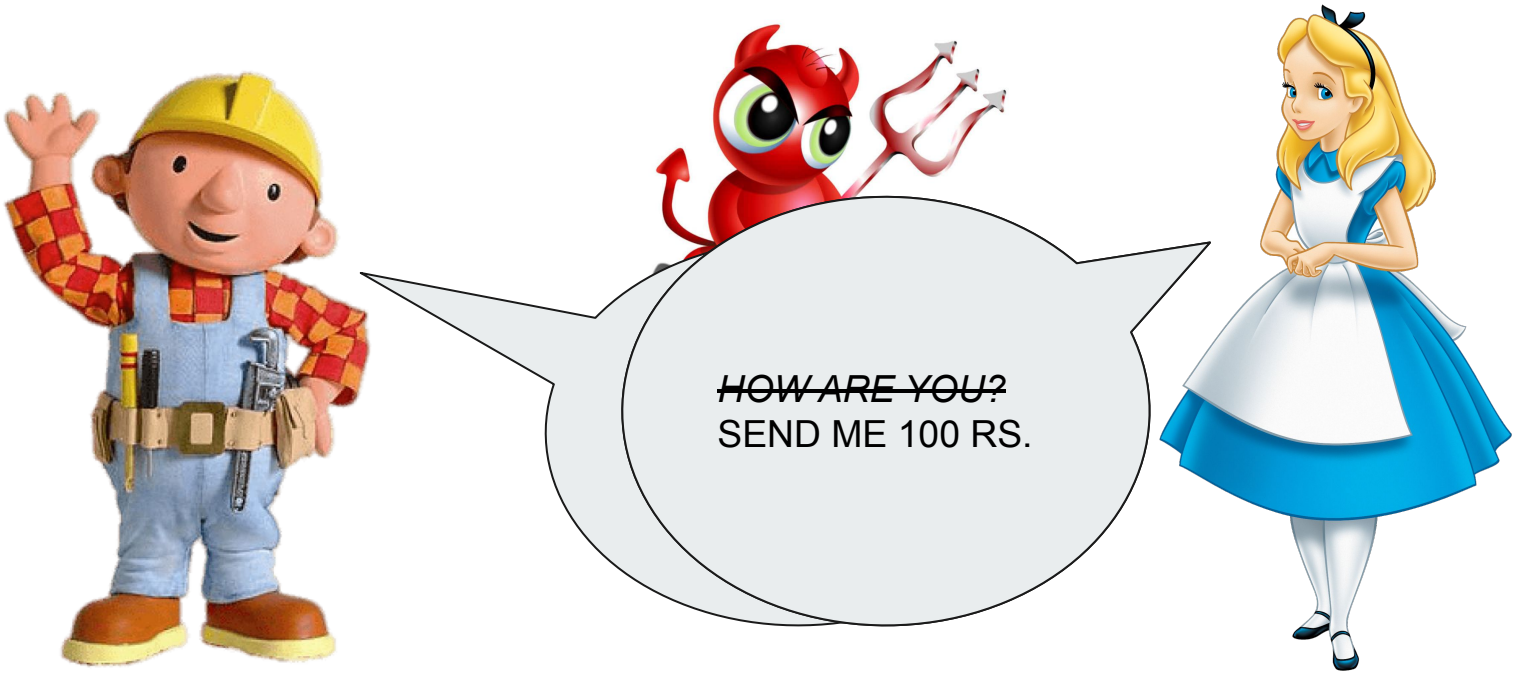
# Cryptography



# Cryptography



# Cryptography



# History of Cryptography

- Earliest known is Scytale Cipher
  - Used by Spartans
  - *Transposition cipher*

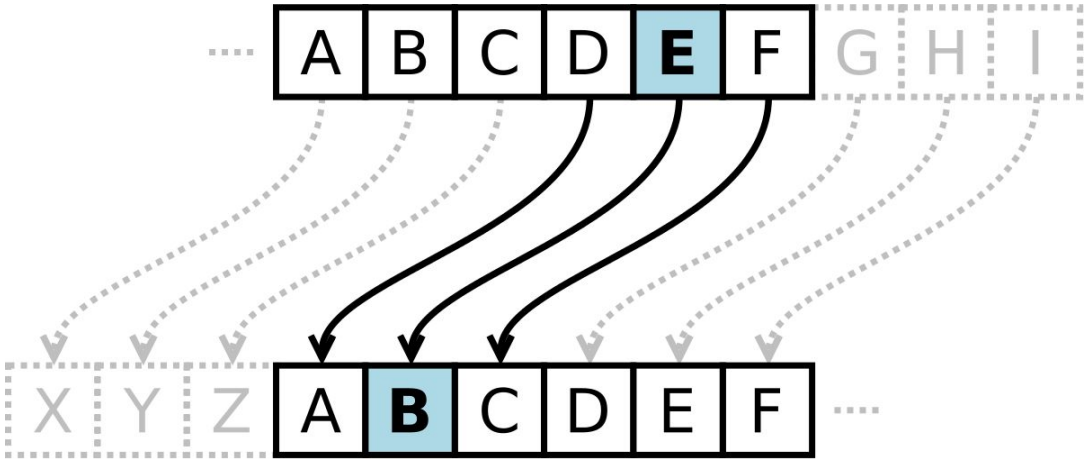
# Transposition Cipher Example

Decrypt: ITGIIAJKCILUIUSESNRSMOEYPAJSTM

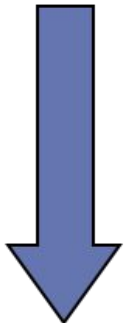
| A | U | T | H | O | R |
|---|---|---|---|---|---|
| I | A | M | J | U | S |
| T | J | O | K | I | N |
| G | S | E | C | U | R |
| I | T | Y | I | S | S |
| I | M | P | L | E | |

# History of Cryptography

- Caesar Cipher
  - Substitution Cipher
  - Used a key (0 to 25) that indicates no. of letters to shift before replacing




DWWDFN EULGJH DW GDZQ



ATTACK BRIDGE AT DAWN

# Simple Substitution Cipher

- Use keywords followed by remaining letters
- Suppose the keyword is ZEBRAS
  - Substitution:

    Plaintext alphabet `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

    Ciphertext alphabet `ZEBRASCDFGHIJKLMNOPQTUVWXY`
- Decipher

  FZJQDAHFIIAO

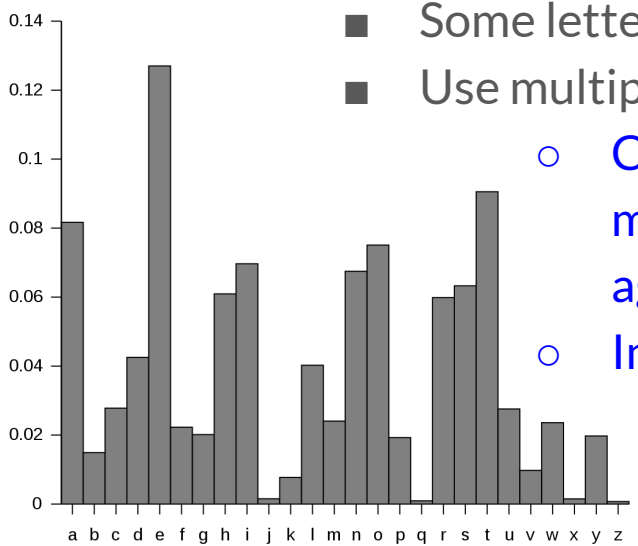
  SIAA ZQ LKBA. VA ZOA RFPBLUAOAR!

# Random Substitution Cipher

- Generate random one-to-one mapping between characters
- A → B, B → E, C → X, D → A, and so on
- Not a constant key shift
- The mapping shared between the parties (symmetric key cryptography)
- Brute-force attack?

# Random Substitution Cipher

- Generate random one-to-one mapping between characters
- A → B, B → E, C → X, D → A, and so on
- **Frequency analysis attack**
  - Some letters are more probable to occur
  - Use multiple encoded messages to reconstruct text
    - Count the occurrences in the “multiple” encrypted messages that we have received and compare them against the existing probabilities.
    - Improve by using digrams …



# Polyalphabetic Ciphers

- Uses multiple substitution alphabets
- Use different monoalphabetic substitutions as one progresses through the message
- Key properties
  - A set of related monoalphabetic substitution rules is used
  - A key determines which particular rule is chosen for a given transformation

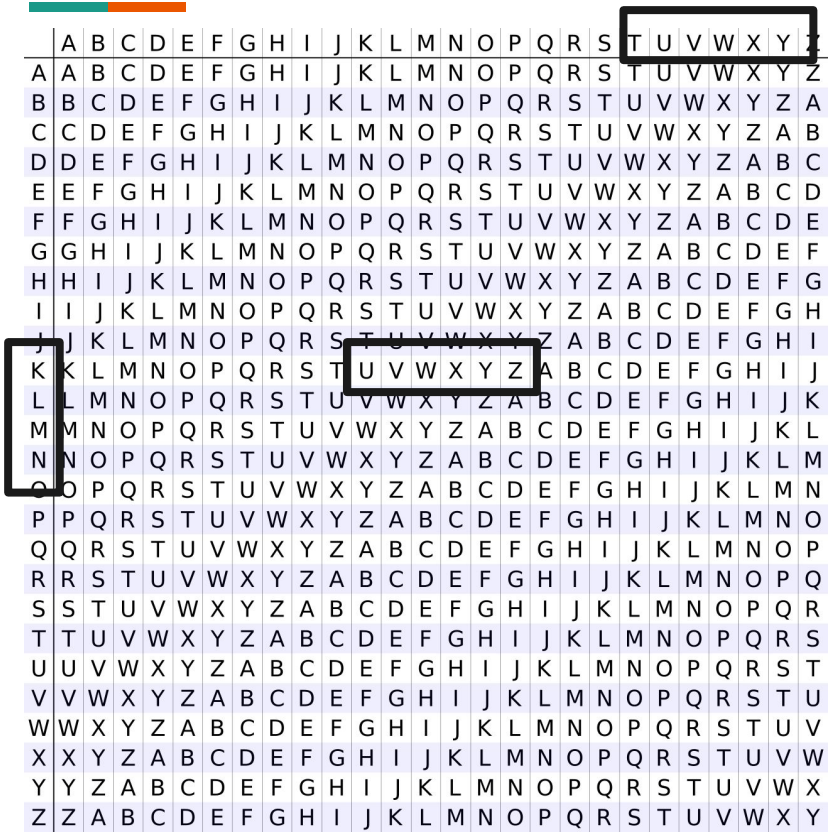
- Enigma (WWII)

# Vigenere Cipher

- Applies a different variant of the Caesar cipher on each letter depending on a key
- The key gives the shift for each letter starting with a = 0 (no shift)
- The key “decrypt” provides the following shifts:

  d = 3; e = 4; c = 2; r = 17; y = 24; p = 15; t = 19

# Vigenere Cipher



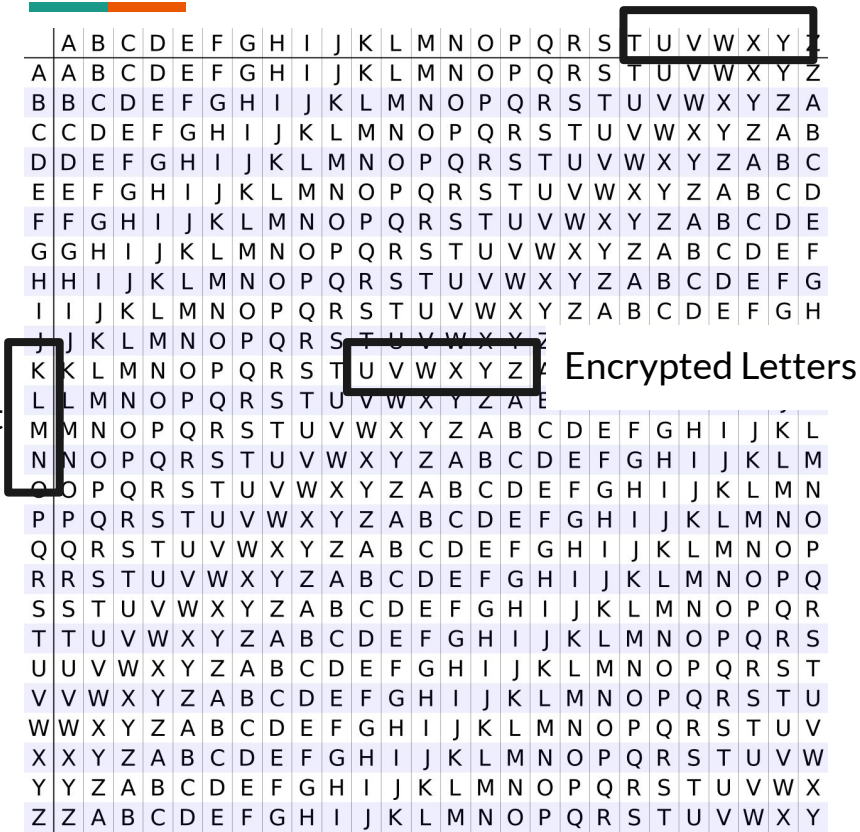
| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T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

IAMJUSTACLOWN

DECRYPTDECRYP

# Vigenere Cipher

The Key




IAMJUSTACLOWN

DECRYPTDECRYP

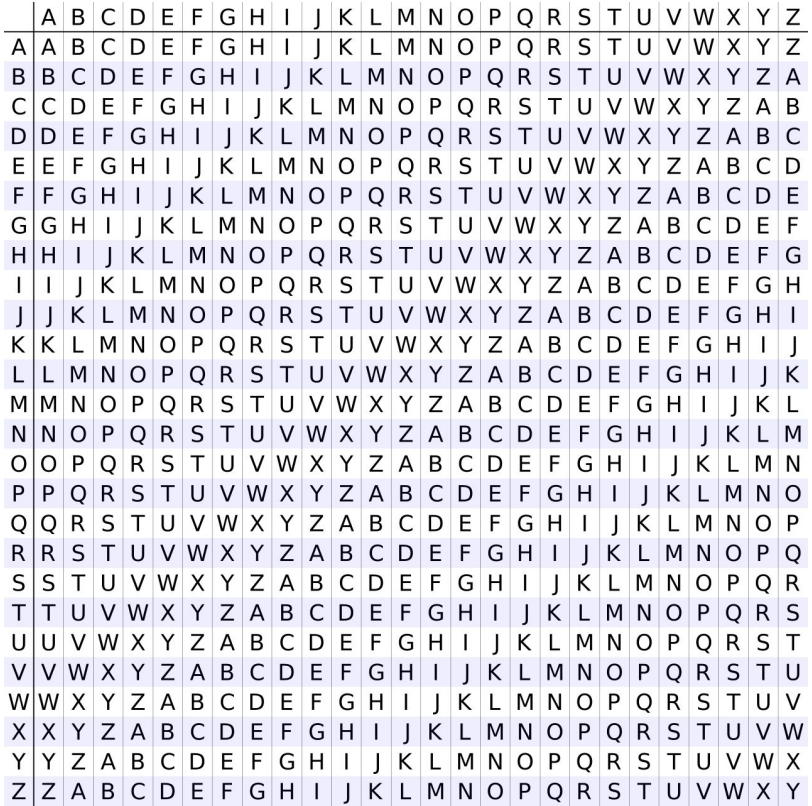
# Vigenere Cipher

**Decrypt this:**

Wmrpnwff hto ngh jrgpnl hii ntpzss

**Key is :**

Bellaso



| | 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 |

# Vigenere Cipher

```
Key:         ABCDABCDABCDABCDABCDABCDABCD
Plaintext:   cryptoisshortforcryptography
Ciphertext:  CSASTPKVSIQUTGQUCSASTPIUAQJB
```

# Vigenere Cipher

- Autotext / Autokey
  - Pad the key with the plaintext, rather than repetitions of the key
    - Decryptyouare
    - Still vulnerable to frequency analysis
    - Can exploit statistical properties if fragment of ciphertext recovered large enough

# Vigenere Cipher

- Autotext
  - Pad the key with the plaintext, rather than repetitions of the key
    - Decryptyouare
    - Still vulnerable to frequency analysis
    - Can exploit statistical properties if fragment of ciphertext recovered large enough
- Use a key as long as the text and statistically independent (Vernam Cipher)

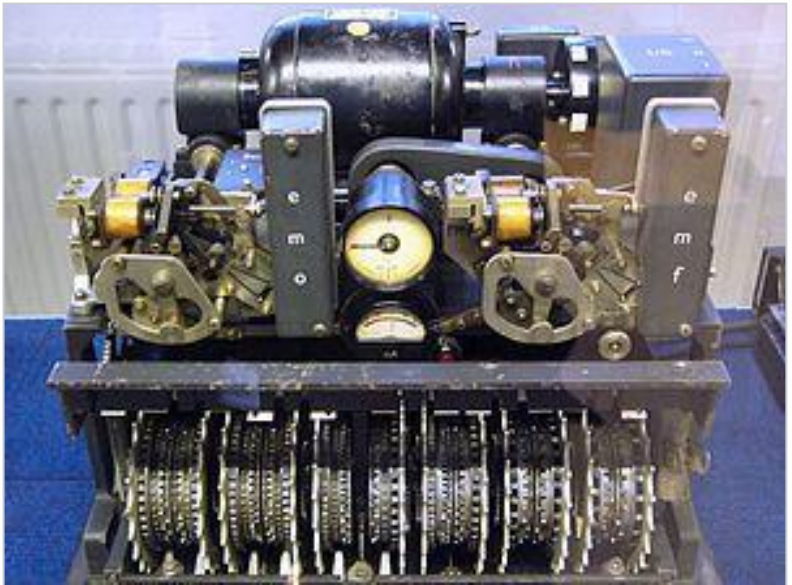
# Vernam Cipher

- Key is as long as the plaintext and statistically independent
- Suppose P is the plaintext, K is the key, then the ciphertext is generated as:

$$C_i = P_i \oplus K_i$$

# One-time Pad

- Proposed during WW1 (used in Cold War, too)
- Truly random key
- Key as long as the plaintext
- Never reused in whole or part
- Kept secret



# One-time Pad

- Because the key is truly random, the same ciphertext can map into any plaintext
- So, one-time pad is invulnerable to cryptanalysis

```
C:ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
K:pxlmvmsydoftyrvzwc tnlebnecvgdupahfzzlmnyih
P:mr mustard with the candlestick in the hall
```

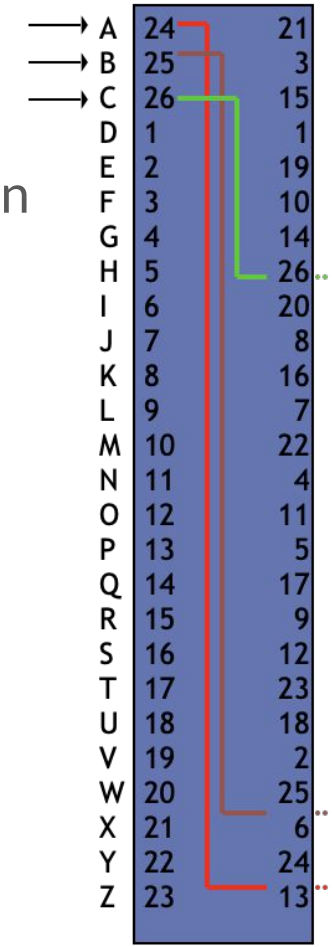
```
C:ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
K:mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt
P:miss scarlet with the knife in the library
```

# One-time Pad

- True randomness extremely difficult!
  - Computers can’t do it
- Impractical for large volumes of data
- Approximations are needed
  - Rotor machines

# Rotor Machines

Use multi-stage encryption

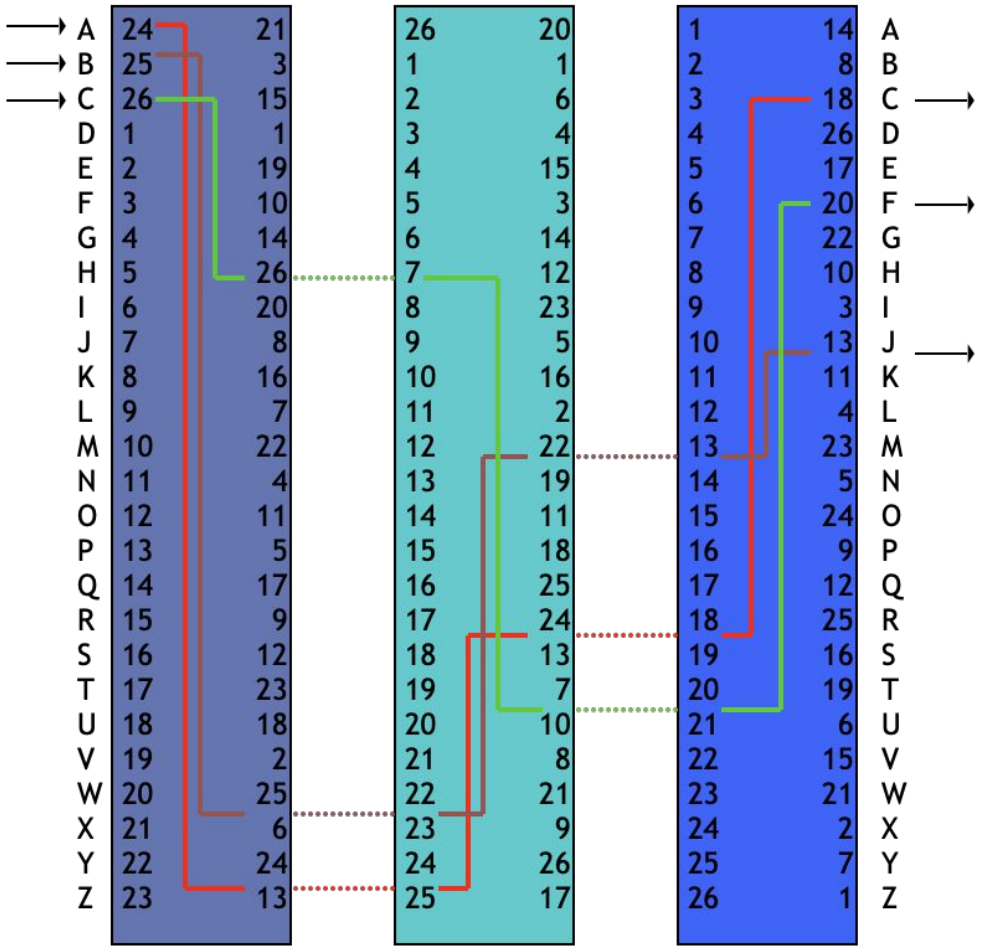


# Rotor Machines

- Use multi-stage encryption
- Each stage consists of a rotor, that performs a monoalphabetic substitution
- Once a key is pressed the rotor shifts by one position
- So, for one rotor, polyalphabetic substitution of period 26
- Power is in using multiple rotors
  - Once the first rotor has completed a full revolution, the second rotor advances by one pin, and so forth
- Widely used in Germany (WWII)

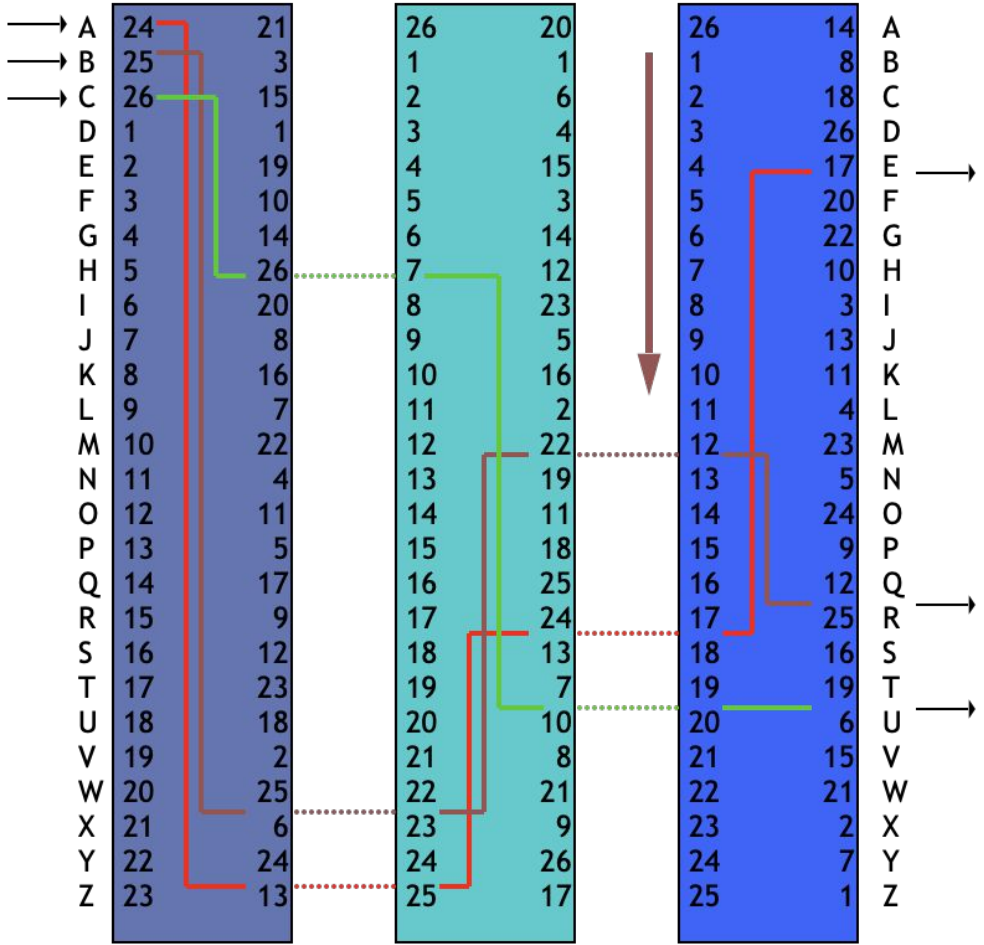
# Rotor Machines

Before 1st Keystroke



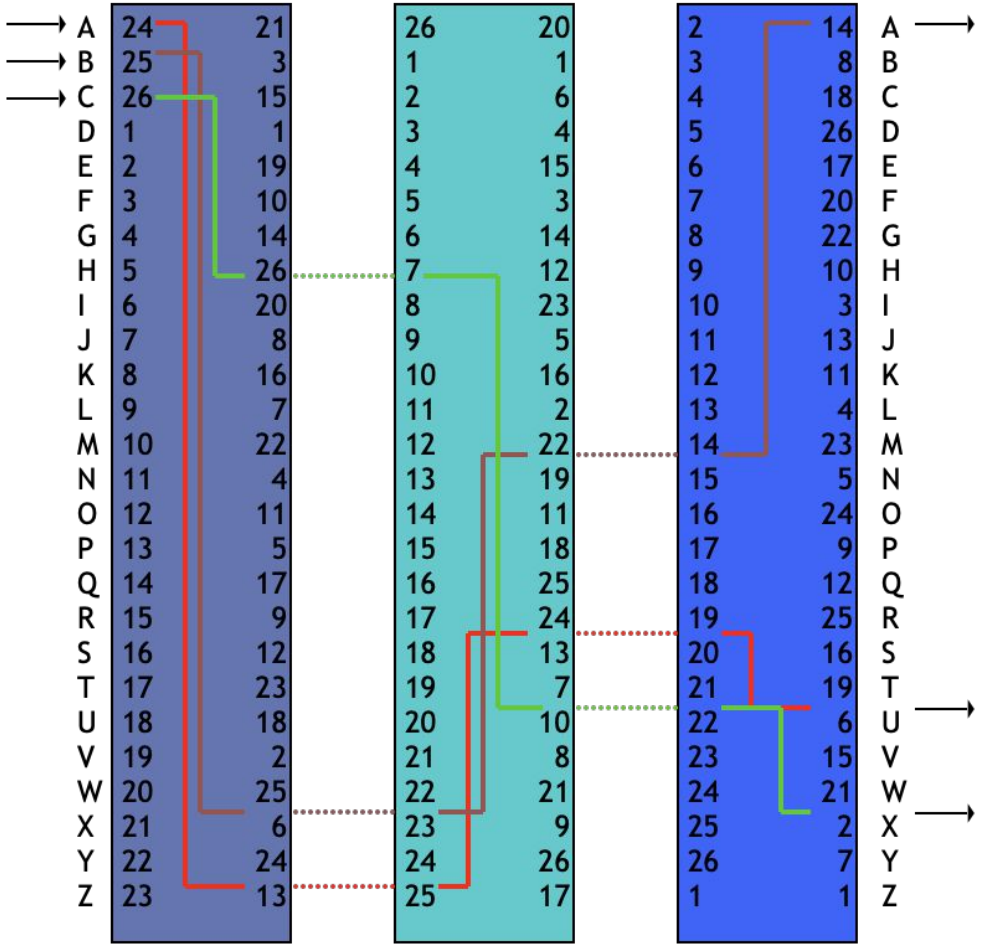
# Rotor Machines

After 1st Keystroke



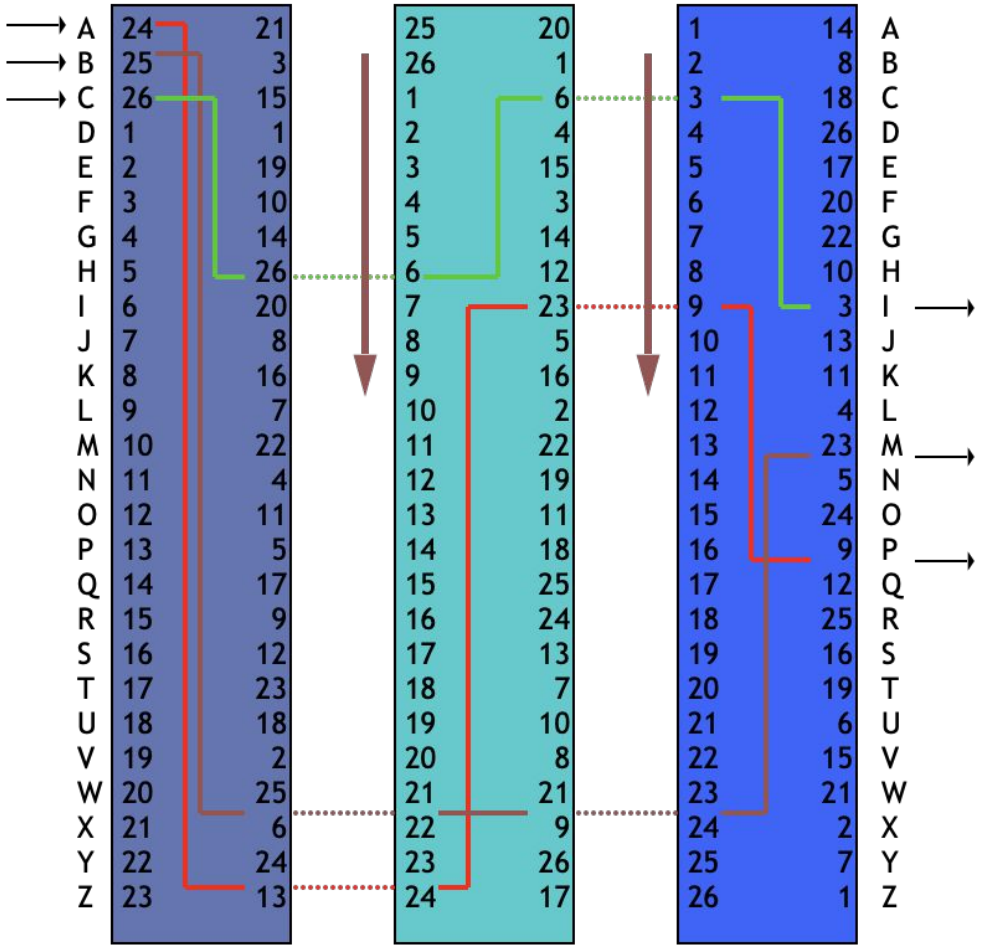
# Rotor Machines

Before 26th Keystroke



# Rotor Machines

After 26th Keystroke



# Rotor Machines

- Achieve randomness of the key by multiple stages of substitution
  - Deterministic, but with a very large period
- 3 stages:
  - 26x26x26 = 17,576 substitution alphabets used before repetition
- 5 stages
  - 26x26x26x26x26 = 11,881,376 substitution alphabets

David Kahn: “A period of that length thwarts any practical possibility of a straightforward solution on the basis of letter frequency. This general solution would need about 50 letters per cipher alphabet, meaning that all five rotors would have to go through their combined cycle 50 times. The ciphertext would have to be as long as all the speeches made on the floor of the Senate and the House of Representatives in three successive sessions of Congress. No cryptanalyst is likely to bag that kind of trophy in his lifetime; even diplomats, who can be as verbose as politicians, rarely scale those heights of loquacity.”

# Rotor Machines

- Achieve randomness of the key by multiple stages of substitution
  - Deterministic, but with a very large period
- 3 stages:
  - 26x26x26 = 17,576 substitution alphabets used before repetition
- 5 stages
  - 26x26x26x26x26 = 11,881,376 substitution alphabets
- Why are rotor machines important?
  - Basis for all multi-stage encryption ciphers, e.g., DES (most widely used cipher)

# Cryptography - An Exercise