# Caesar Cipher

- Mathematically, map letters to numbers:

```
a, b, c, ..., x,  y,  z
0, 1, 2, ..., 23, 24, 25
```

- Then the general Caesar cipher is:

  $c = E_K(p) = (p + k) \bmod 26$

  $p = D_K(c) = (c - k) \bmod 26$

- Can be generalized with any alphabet.

# Cryptanalysis of Caesar Cipher

- Key space:  {0, 1, ..., 25}
- Vulnerable to brute-force attacks.
- E.g., break ciphertext "UNOU YZGZK“

- Need to recognize it when have the plaintext
- What if the plaintext is written in Swahili?

# Playfair Cipher

- Not even the large number of keys in a monoalphabetic cipher provides security.

.

- One approach to improving security is to encrypt Two letters at a time.
- The **Playfair Cipher** is the best known such cipher.
- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair.

# Playfair Key Matrix

- Use a 5 x 5 matrix.
- Fill in letters of the key (w/o duplicates).
- Fill the rest of matrix with other letters.
- E.g., key = MONARCHY.

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

# Encrypting and Decrypting

Plaintext is encrypted two letters at a time.

1. If a pair is a repeated letter, insert filler like 'X'.
2. After inserting the bogus letter the size of plain text must be ,otherwise add bogus(same or other) letter to make it even.
3. If both letters fall in the same row, replace each with the letter to its right (circularly).
4. If both letters fall in the same column, replace each with the the letter below it (circularly).
5. Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair.

# Hill cipher

- Key K is square matrix of size m × m (inverse must exists)
- Plain text of size l × m, where l is no. of blocks
- Example: “code is ready”

  Plain text is 3 × 4 matrix
- Cipher text C = (P × K) mod 26
- Plain text P= ( C × $K^{-1}$ ) mod 26

# Cryptanalysis

- Objective: to recover the plaintext of a ciphertext or, more typically, to recover the secret key.

.

# Cryptanalytic Attacks

- May be classified by how much information needed by the attacker:
  - Ciphertext-only attack
  - Known-plaintext attack
  - Chosen-plaintext attack
  - Chosen-ciphertext attack

# Brute-Force Attack

- Try every key to decipher the ciphertext.
- On average, need to try half of all possible keys
- Time needed proportional to size of key space

| Key Size (bits) | Number of Alternative Keys | Time required at 1 decryption/μs | Time required at $10^6$ decryptions/μs |
|---|---|---|---|
| 32 | $2^{32} = 4.3 \times 10^9$ | $2^{31}$ μs = 35.8 minutes | 2.15 milliseconds |
| 56 | $2^{56} = 7.2 \times 10^{16}$ | $2^{55}$ μs = 1142 years | 10.01 hours |
| 128 | $2^{128} = 3.4 \times 10^{38}$ | $2^{127}$ μs = $5.4 \times 10^{24}$ years | $5.4 \times 10^{18}$ years |
| 168 | $2^{168} = 3.7 \times 10^{50}$ | $2^{167}$ μs = $5.9 \times 10^{36}$ years | $5.9 \times 10^{30}$ years |
| 26 characters (permutation) | $26! = 4 \times 10^{26}$ | $2 \times 10^{26}$ μs = $6.4 \times 10^{12}$ years | $6.4 \times 10^6$ years |

Frequency of occurrence of letters in English text:

E-12.7 T-9.1 A-8.2.....J-0.02 Q-0.01 X-0.01 Z-0.01

Digram:

TH,HE,IN,ER,AN,RE,ED,ON,ES,ST,EN,AT,TO,NT,HA,ND,OD,EA,NG,AS,OR,
TL,IS,ET,IT,AR,TE,SE,HL,OF

Trigram: THE ,ING,AND,HER,ERE,ENT,THA,NTHWAS,ETH,POR,DTH

# Ciphertext-only attack

- Given: a ciphertext c
- Q: what is the plaintext m?
- An encryption scheme is completely insecure if it cannot resist ciphertext-only attacks.

# Known-plaintext attack

- Given: $(m_1,c_1)$, $(m_2,c_2)$, ..., $(m_k,c_k)$ and a new ciphertext c.

- Q: what is the plaintext of c?
- Q: what is the secret key in use?

# Chosen-plaintext attack

- Given: $(m_1,c_1)$, $(m_2,c_2)$, ..., $(m_k,c_k)$, where $m_1, m_2, ..., m_k$ are chosen by the adversary; and a new ciphertext c.

- Q: what is the plaintext of c, or what is the secret key?

# Example: chosen-plaintext attack

- In 1942, US Navy cryptanalysts discovered that Japan was planning an attack on “AF”.
- They believed that “AF” means Midway island.
- Pentagon didn’t think so.
- US forces in Midway sent a plain message that their freshwater supplies were low.
- Shortly, US intercepted a Japanese ciphertext saying that “AF” was low on water.
- This proved that “AF” is Midway.

# Chosen-ciphertext attack

- Given: $(m_1,c_1)$, $(m_2,c_2)$, ..., $(m_k,c_k)$, where $c_1, c_2, ..., c_k$ are chosen by the adversary; and a new ciphertext c.

- Q: what is the plaintext of c, or what is the secret key?