Cryptography
CS 555

Topic 2: Historical Ciphers (& How to Break Them)

Symmetric Key Encryption

- What cryptography has historically been all about (Pre 1970)
- Two parties (sender and receiver) share secret key

- Sender uses key to encrypt (“scramble”) the message before transmission
- Receiver uses the key to decrypt (“unscramble”) and recover the original message

Encryption: Basic Terminology

- Plaintext
  - The original message m
- Plaintext Space (Message Space)
  - The set $\mathcal{M}$ of all possible plaintext messages
  - Example 1: $\mathcal{M} = \{\ 'attack',\ 'retreat',\ 'hold\ current\ position'\}$
  - Example 2: $\mathcal{M} = \{0,1\}^n$ - all $\mathrm{n} - \mathrm{bit}$ messages
- Ciphertext $\mathrm{c} \in \mathcal{C}$
  - An encrypted ("scrambled") message $\mathrm{c} \in \mathcal{C}$ (ciphertext space)
- Key/Keyspace $\mathrm{k} \in \mathcal{K}$

Private Key Encryption Syntax

- Message Space: $\mathcal{M}$
- Key Space: $\mathcal{K}$
- Three Algorithms
  - $\mathrm{Gen}(R)$ (Key-generation algorithm)
    - Input: Random Bits R
    - Output: Secret key $\mathrm{k} \in \mathcal{K}$
  - $\mathrm{Enc}_{\mathrm{k}}(m)$ (Encrytpion algorithm)
    - Input: Secret key $\mathrm{k} \in \mathcal{K}$ and message $\mathrm{m} \in \mathcal{M}$
    - Output: ciphertext *c*
  - $\mathrm{Dec}_{\mathrm{k}}(c)$ (Decryption algorithm)
    - Input: Secret key $\mathrm{k} \in \mathcal{K}$ and a ciphertex c
    - Output: a plaintext message $\mathrm{m} \in \mathcal{M}$
- Invariant: $\mathrm{Dec}_{\mathrm{k}}(\mathrm{Enc}_{\mathrm{k}}(\mathrm{m}))=\mathrm{m}$

Typically picks $\mathrm{k} \in \mathcal{K}$ uniformly at random

Trusted Parties (e.g., Alice and Bob) must run Gen in advance to obtain secret k.

Assumption: Adversary does not get to see output of Gen

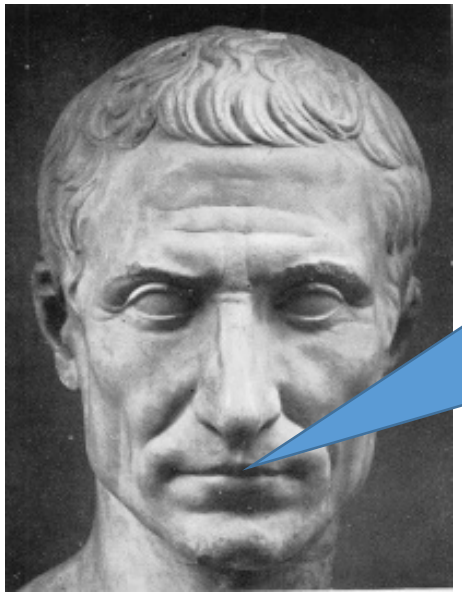
Shift Cipher

- Key Space: $\mathcal{K}$={0,1,…,25}
- Message Space: $\mathcal{M}$={a,b,c,…,z}
- Right Shift Operation
  - $RS_1(a) = b$
  - $RS_1(b) = c$
  - ...
  - $RS_1(z) = ?$
  - $Rs_{i+1}(a)=Rs_i(b)$
- $\mathrm{Enc}_k(m)$
  - Each letter in plaintext message m is right shifted k times RS_k
- Question: what is ciphertext space $\mathcal{C}$?

Shift Cipher

- Key Space: $\mathcal{K}$={0,1,…,25}
- Message Space: $\mathcal{M}$={a,b,c,…,z}*
- Left Shift Operation
  - LS_1(a) = z
  - LS_1(b) = a
  - …
  - LS_1(z) = y
- $\mathrm{Dec}_k(c)$
  - Each letter in ciphertext c is left shifted k times

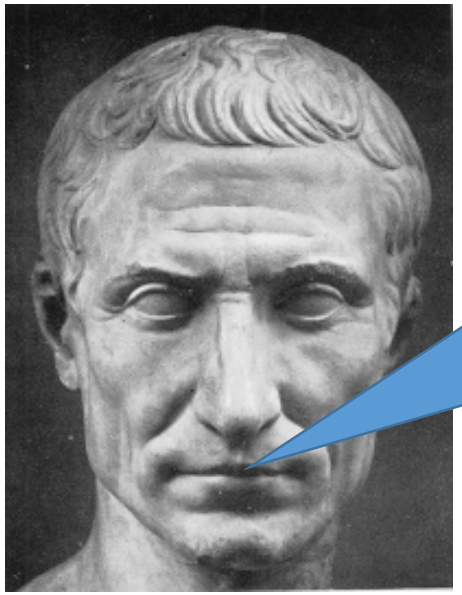
Caesar Cipher



Three shall be the number of thy shifting and the number of thy shifting shall be three. Four shalt thou not shift, neither shift thou two, excepting that thou then proceed to three. Five is right out…..

Caesar adopted the shift cipher with secret key k=3

Caesar Cipher (Example)



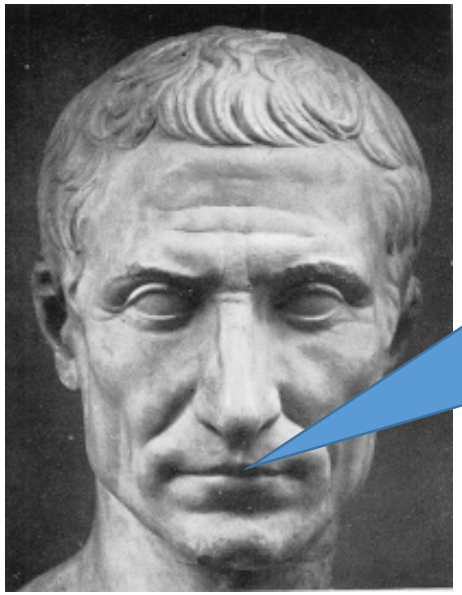
BEGINTHEATTACKNOW

→

EHJLQWKHDWWDFNQRZ

Caesar adopted the shift cipher with secret key k=3

Caesar Cipher (Example)



BEGINTHEATTACKNOW
→
EHJLQWKHDWWDFNQRZ

Immediate Issue: anyone who knows method can decrypt (since k=3 is fixed)

Modern Application: Avoid Spoilers (ROT13)

Harry Potter

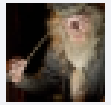
I was shocked and horrified when Snape killed Dumbledore.

Like · Comment · 32 minutes ago ·

26 people like this.

Hagrid Me too!

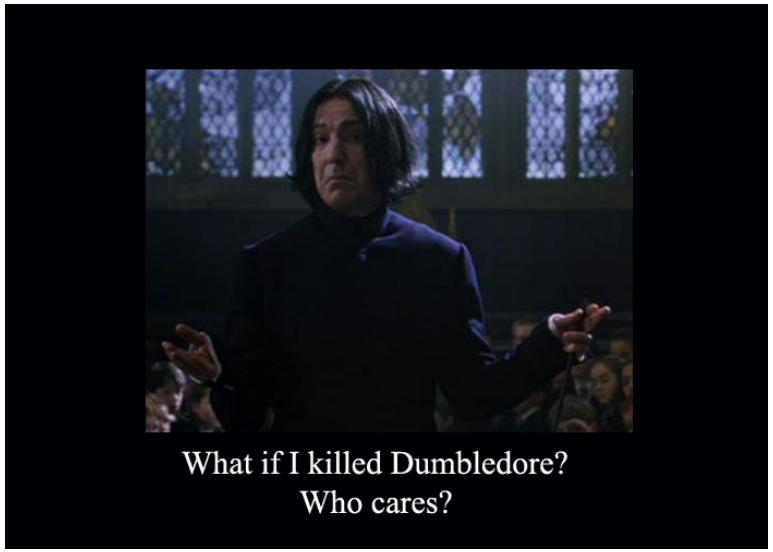
31 minutes ago · Like · 3



Dumbledore Thanks for ruining the plot, jerk!

15 minutes ago · Like · 34

Write a comment ...



Modern Application: Avoid Spoilers (ROT13)

Harry Potter

[ROT13 to avoid spoilers] V jnf fubpxrq naq ubeevsvrq jura Fancr xvyyrq Qhzoyrqber.

Like · Comment · 32 minutes ago ·

20 people like this.

Dumbledore I am dying to find out what will happen, but I will wait to decrypt until after I read the book.

15 minutes ago · Like · 23

Write a comment ...

Shift Cipher: Brute Force Attack

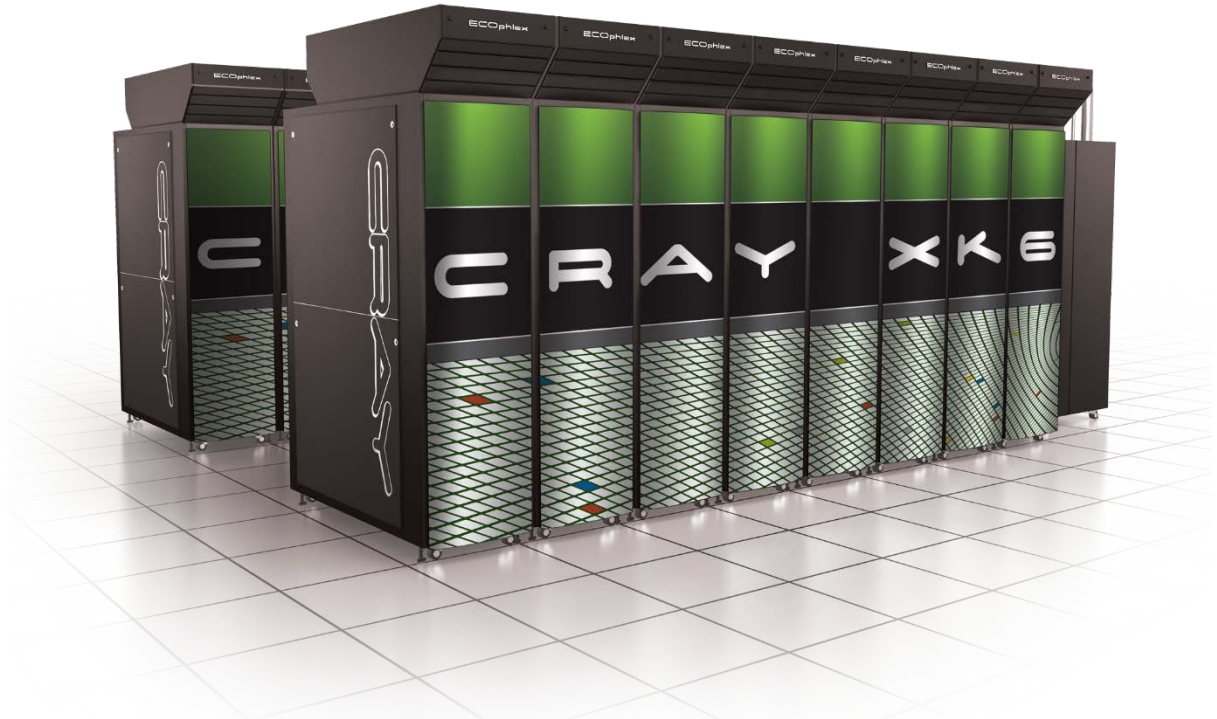
- Ciphertext: “lwxrw ztn sd ndj iwxcz xh gxvwi?”
  - k=1 → m = “mxysx auo te oek jxyda yi hywxj?”
  - k=2 → m=“nyzty bvp uf pfl kyzeb zj izxyk?”
  - k=3 → m=“ozauz cwq vg qgm lzafc ak jayzl?”
  - k=4 → m = “pabva dxr wh rhn mabgd bl kbzam?”
  - k=5 → m=“qbcwb eys xi sio nbche cm lcabn?”
  - k=6 → m=“rcdxc fzt yj tjp ocdif dn mdbco?”

Shift Cipher: Brute Force Attack

- Ciphertext: “lwxrw ztn sd ndj iwxcz xh gxvwi?”
  - …
  - k=7 → m=“sdeyd gau zk ukq pdejg eo necdp?”
  - k=8 → m=“tefze hbv al vlr qefkh fp ofdeq?”
  - k=9 → m = “ufgaf icw bm wms rfgli gq pgefr?”
  - k=10 → m=“vghbg jdx cn xnt sghmj hr qhfgs?”
  - k=11→ m= “which key do you think is right?”
  - k=12→ m= “xijdi lfz ep zpv uijol jt sjhiu?”

Sufficient Key Space Principle

"Any secure encryption scheme *must* have a key space that is sufficiently large to make an exhaustive search attack infeasible."



Sufficient Key Space Principle

"Any secure encryption scheme *must* have a key space that is sufficiently large to make an exhaustive search attack infeasible."

Question 1: How big is big enough? Complicated question….

Question 2: If the key space is large is the encryption scheme necessarily secure?

Substitution Cipher

- Secret key K is permutation of the alphabet
  - Example:
    - 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
    - X E U A D N B K V M R O C Q F S Y H W G L Z I J P T

- Encryption: apply permutation K to each letter in message
  - TELLHIMABOUTME → GDOOKVCXEFLGCD

- Decryption: reverse the permutation

Substitution Cipher

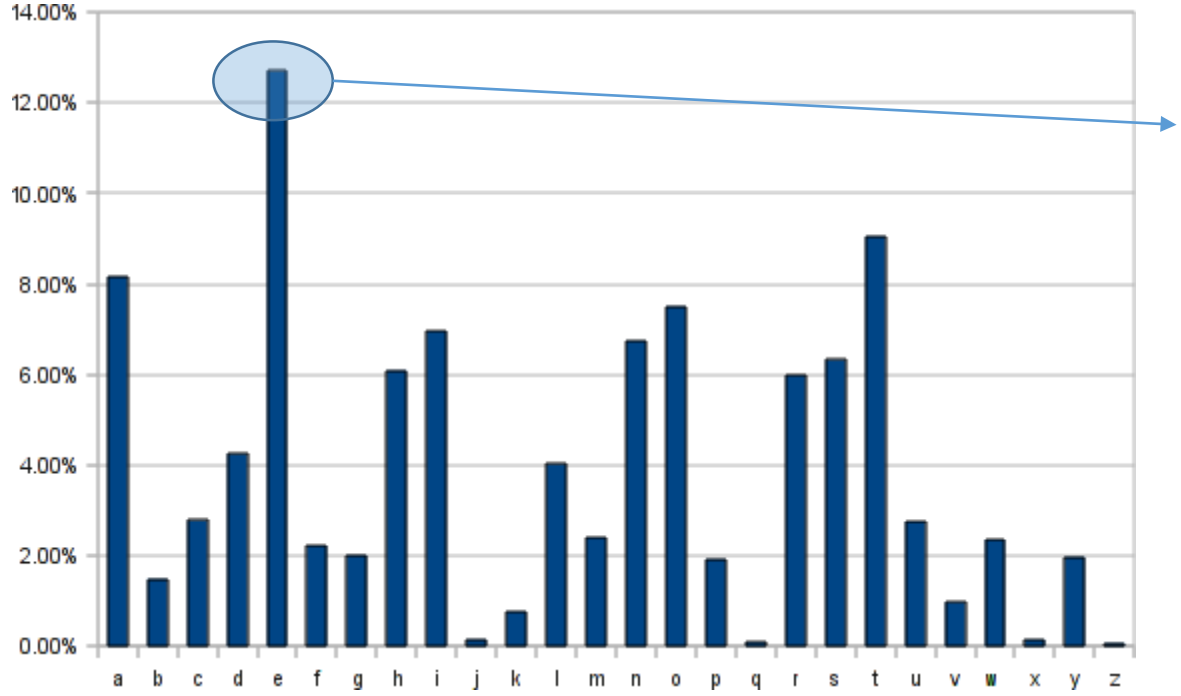
- Secret key K is a permutation of the alphabet
  - Example:
    - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
    - X E U A D N B K V M R O C Q F S Y H W G L Z I J P T

- Question: What is the size of the keyspace $\mathcal{K}$?

$$|\mathcal{K}| = 26! \approx 2^{88}$$

Frequency Analysis

- **Observation 1:** If e is mapped to d then every appearance of e in the plaintext results in the appearance of a d in the ciphertext
- **Observation 2:** Some letters occur much more frequently in English.
- **Observation 3:** Texts consisting of a few sentences tend to have a distribution close to average.



Step 1: Find letter in ciphertext that occurs with frequency > 11%. This letter is probably e…

Vigenere Cipher

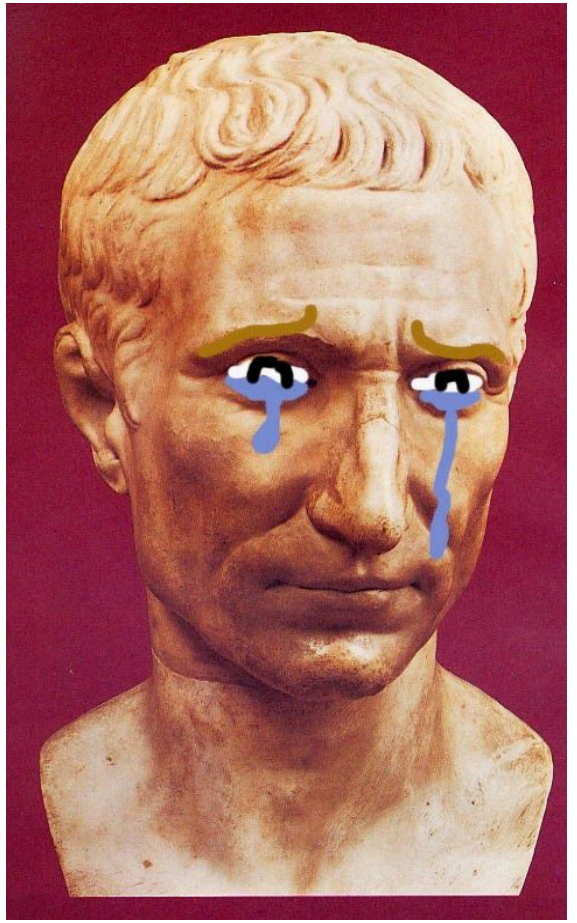
- Generalizes Shift Cipher
- $K=k_1,\ldots,k_t$
- $Enc_K(m)$
  - Shift first letter right k_1 times
  - Shift second letter right k_2 times
  - …
  - Shift t^{th} letter right k_t times
  - Shift $t+1^{st}$ letter right k_1 times
  - …
- **Question:** Size of key-space?
- Answer: 26^t (brute force may not be useful)

Vigenere Cipher

- Still vulnerable to frequency analysis
- Good guess: Select $K=k_1,\ldots,k_t$ to maximize number of e's in resulting ciphertext
  - See Katz and Lindell 1.3 for even more sophisticated heuristics.
- Works if the initial message m is long enough
- Vigenere is perfectly secure if the message m is at most t letters long.

Conclusions

- Designing secure ciphers is hard
- Vigenere remained “unbroken” for a long time
- Complex schemes are not secure
- All historical ciphers have fallen



Principles of Modern Cryptography

- Need formal definitions of “security”

  If you don’t understand what you want to achieve, how can you possibly know when (or if) you have achieved it?

  - Attempt 1: Impossible for attacker to recover secret key K
    - $\mathrm{Enc}_k(m) = m$
  - Attempt 2: Impossible for attacker to recover entire plaintext from ciphertext?
    - Ok to decrypt 90% of message?
  - Attempt 3: Impossible for attacker to figure out any particular character of the plaintext from the ciphertext?
    - [Too Weak] Does employee make more than $100,000 per year?
    - [Too Strong] Lucky guess? Prior Information? (e.g., letters always begin “Dear ….”)

Principles of Modern Cryptography

- Need formal definitions of “security”

  If you don’t understand what you want to achieve, how can you possibly know when (or if) you have achieved it?

  - Final Attempt: Regardless of information an attacker *already* has, a ciphertext should leak no *additional information* about the underlying plaintext.
    - This is the “*right*” approach
    - Still need to *formalize* mathematically

- Security definition includes *goal* and *threat-model*

Principles of Modern Cryptography

- Proofs of Security are critical
  - Iron-clad guarantee that attacker will not succeed (relative to definition/assumptions)
- Experience: intuition is often misleading in cryptography
  - An “intuitively secure” scheme may actually be badly broken.

- Before deploying in the real world
  - Consider definition/assumptions in security definition
  - Does the threat model capture the attackers true abilities?

Coming Up…

- Perfect Secrecy

- Before Next Class
  - Read: Katz and Lindell Chapter 2
  - (Assumes familiarity with basic probability theory, see Appendix A.3)