CS557: Cryptography

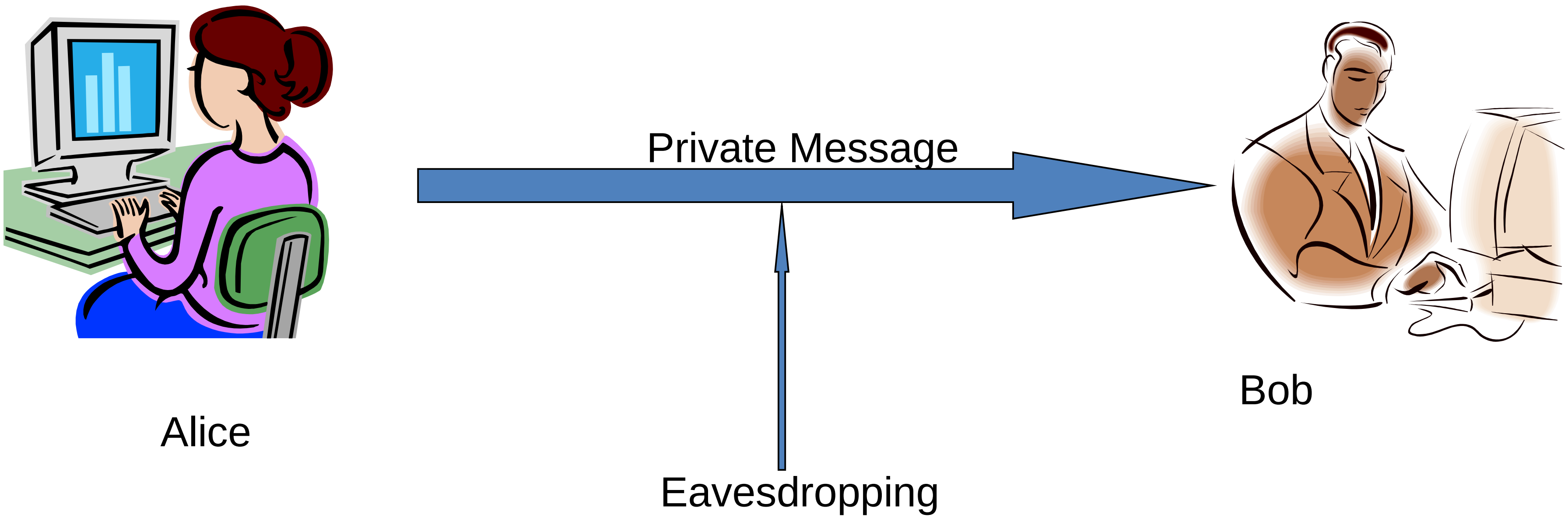
Classical Ciphers

S. Tripathy
IIT Patna

Cryptography

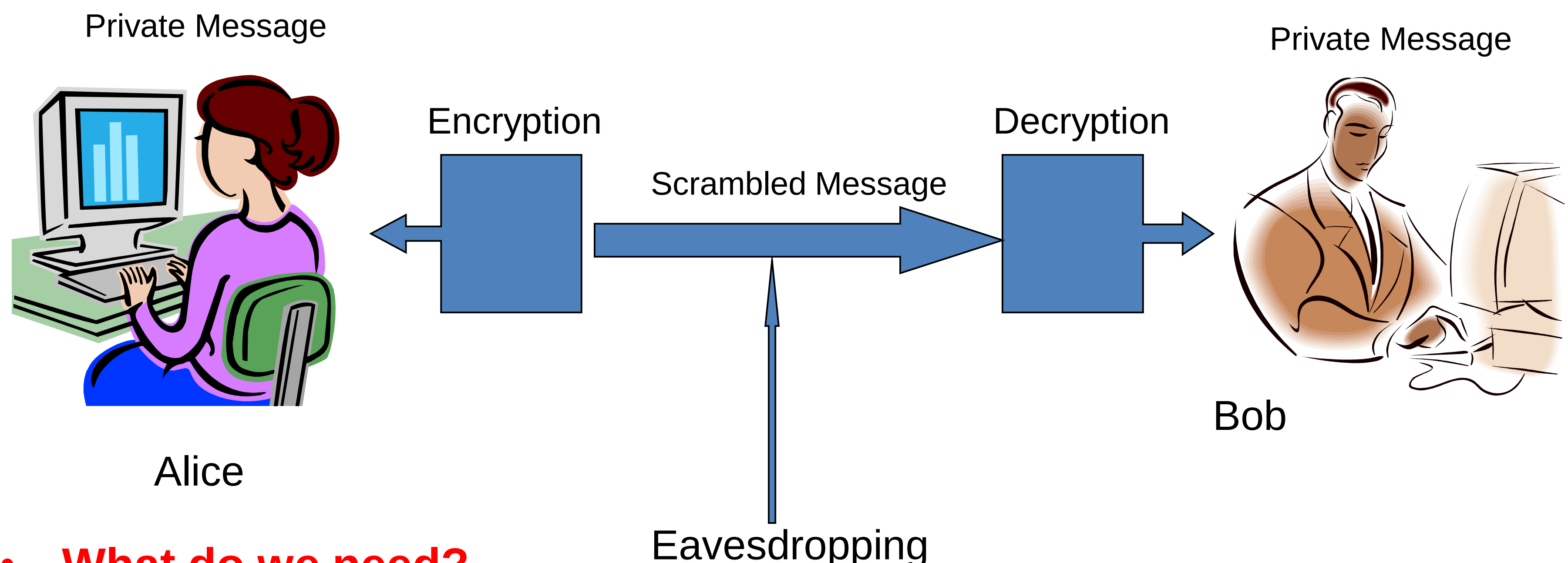
- Cryptography is an indispensable tool to provide security
  - Confidentiality, Integrity, Authentication
  - Encryption
  - Hash Function
  - MAC
  - Digital Signature

The Problem



- **What do we need?**

The Solution

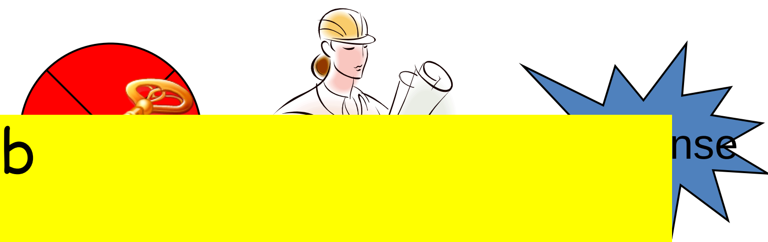


- **What do we need?**
- Alice and Bob want to be able to encrypt/decrypt easily
- But no one else should be able to decrypt

- **How do we do this?**

Keys!

Using Keys



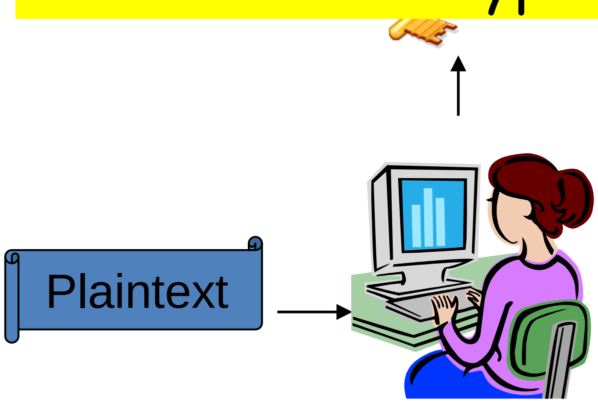
Alice wants to send message X to Bob

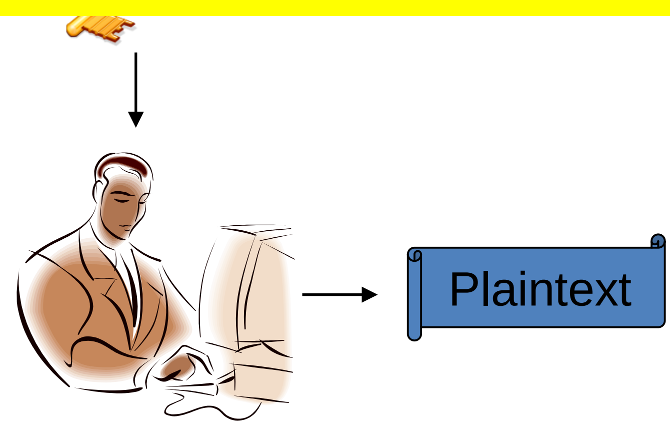
Eve is on the wire, listening to communications.

Alice and Bob share a key K

Alice encrypts X into Y using K Alice sends Y to Bob

Bob decrypts Y back X using K





Definition of Cryptosystem

A cryptosystem is a tuple (P,C,K,E,D) such that:

1. P is a finite set of possible plaintexts
2. C is a finite set of possible ciphertexts
3. K is a finite set of possible keys (keyspace)
4. For every k, there is an encryption function $e_k < E$ and decryption function $d_k < D$ such that $d_k(e_k(x)) = x$ for all plaintexts x.

Encryption function assumed to be injective

Encrypting a message:

$x = x_1\ x_2 \ldots x_n \rightarrow e_k(x) = e_k(x_1)\ e_k(x_2) \ldots e_k(x_n)$

Properties of Cryptosystems

- Encryption and decryption functions can be efficiently computed
- Given a ciphertext, it should be difficult for an opponent to identify the encryption key and the plaintext
  - The key space must be large enough!
  - Otherwise, easy to iterate through all keys

Cryptanalysis

Kerckhoff's Principle:

- The opponent knows the cryptosystem being used

Objective of an attacker:

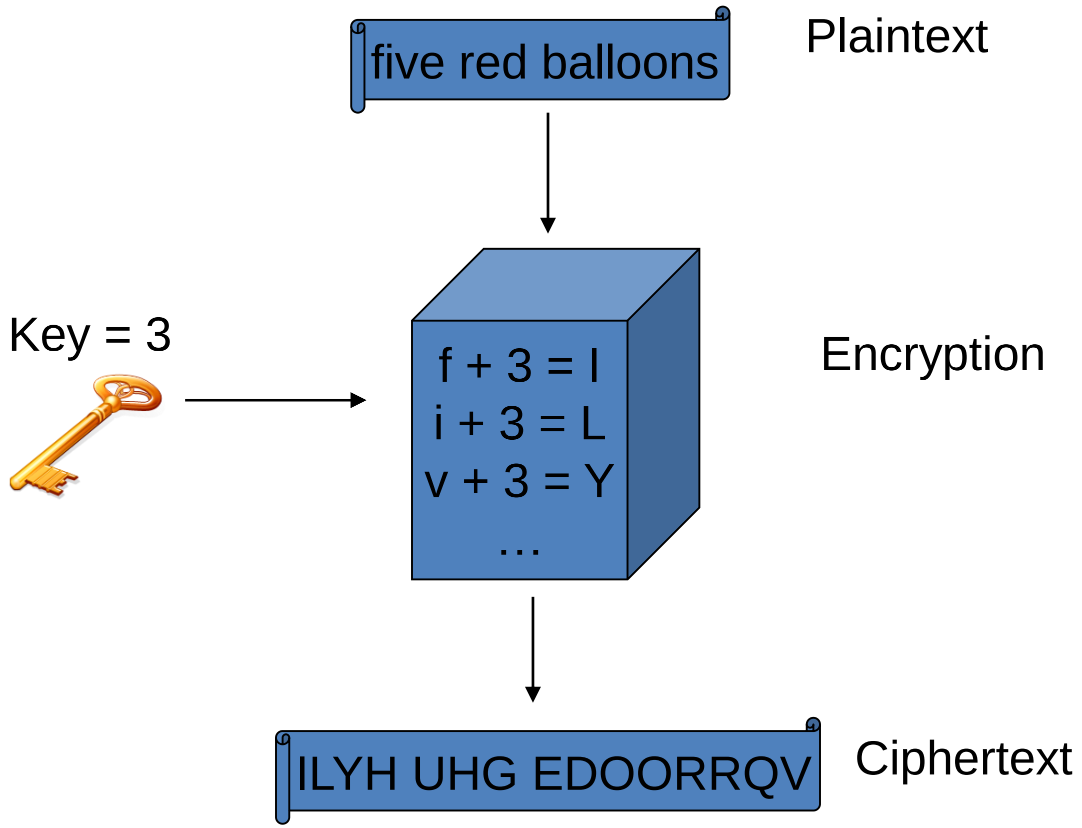
- Identify secret key used to encrypt a ciphertext

Different models are considered:

- Ciphertext only attack
- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack

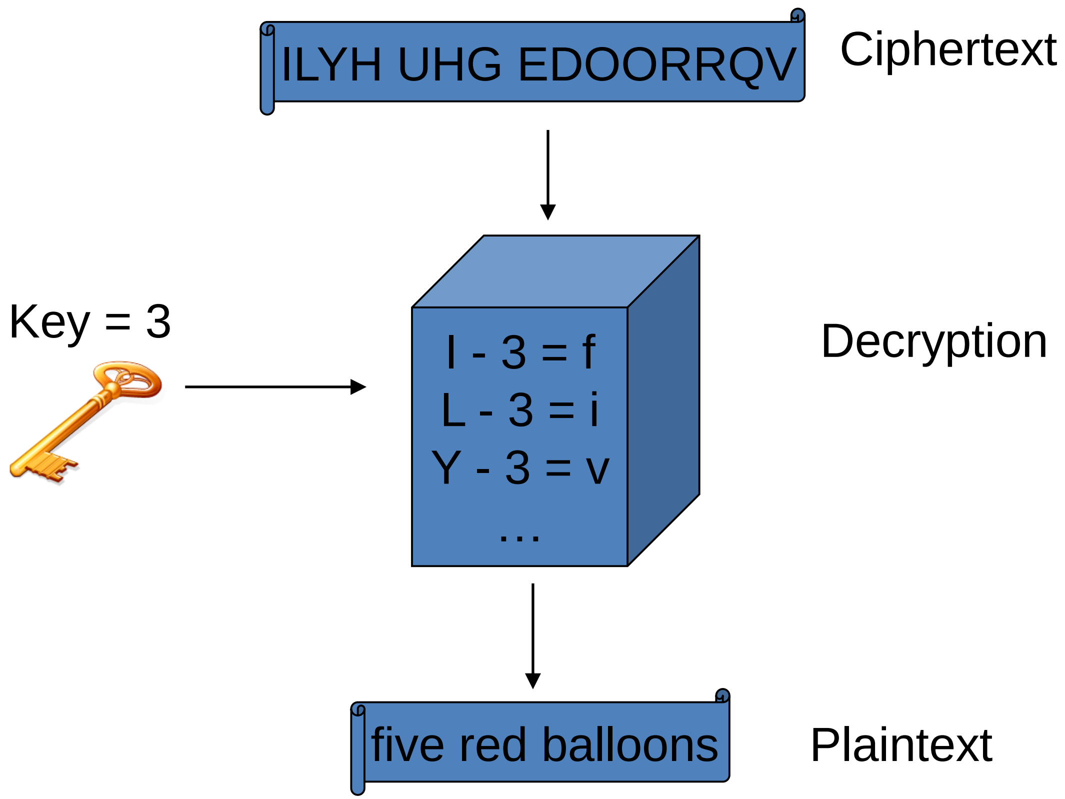
The Shift Cipher

- “shift” each letter over by a certain amount



The Shift Cipher cont.

- To decrypt, just subtract the key



What's wrong with the shift cipher?

- Not enough keys!
- If we shift a letter 26 times, we get the same letter back
  - A shift of 27 is the same as a shift of 1, etc.
  - So we only have 25 keys (1 to 25)
- Eve just tries every key until she finds the right one

The Substitution Cipher

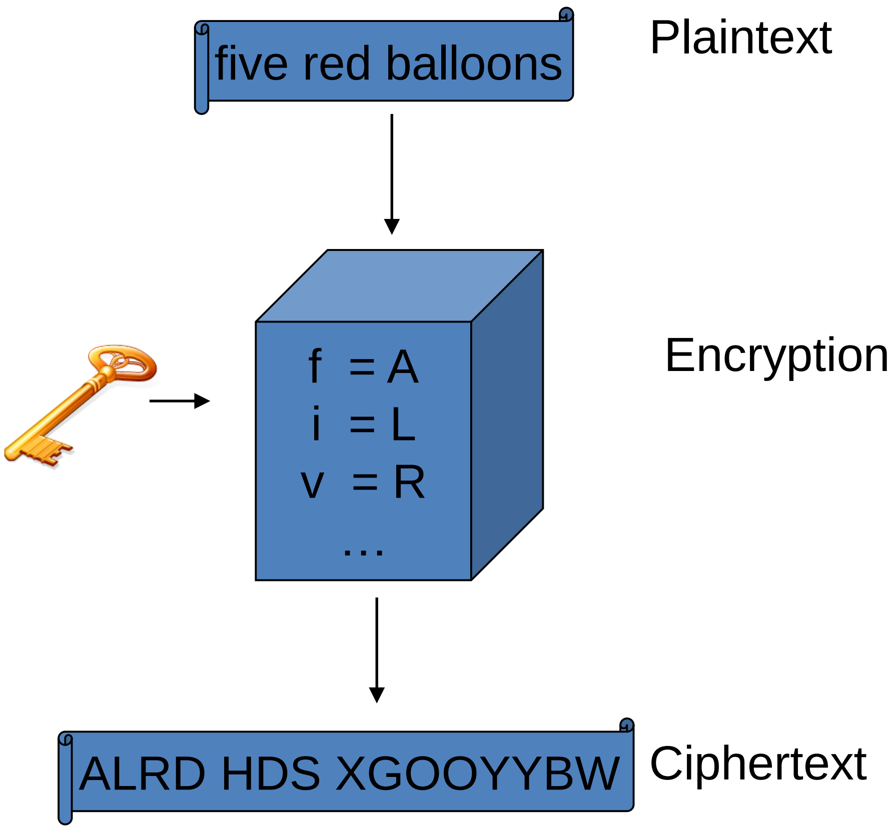
- Rather than having a fixed shift, change every plaintext letter to an arbitrary ciphertext letter

Plaintext	Ciphertext
a	G
b	X
c	N
d	S
e	D
…	…
z	Q

The Substitution Cipher cont.

Key =

a	G	n	B
b	X	o	Y
c	N	p	Z
d	S	q	P
e	D	r	H
f	A	s	W
g	F	t	I
h	V	u	J
i	L	v	R
j	M	w	U
k	C	x	K
l	O	y	T
m	E	z	Q



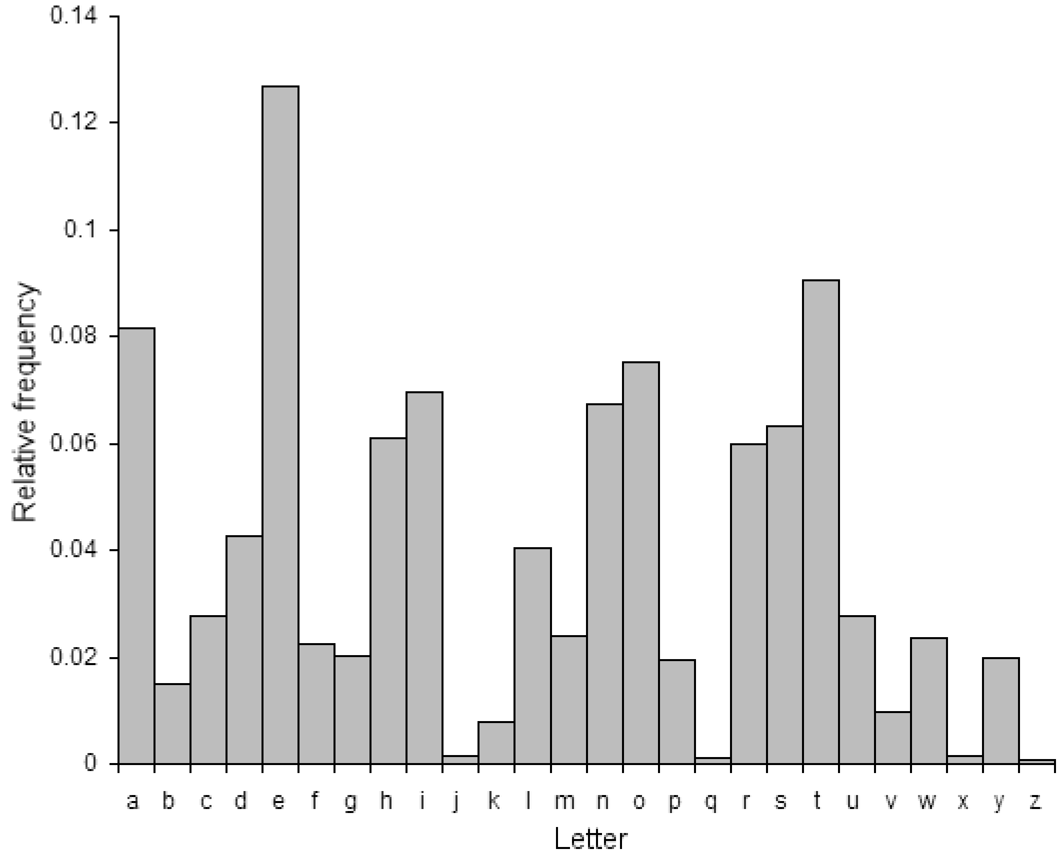
The Substitution Cipher cont.

- To decrypt we just look up the ciphertext letter in the table and then write down the matching plaintext letter

- How many keys do we have now?
  - A key is just a permutation of the letters of the alphabet
  - There are 26! permutations
    - 403291461126605635584000000
- What's wrong with this substitution Cipher?

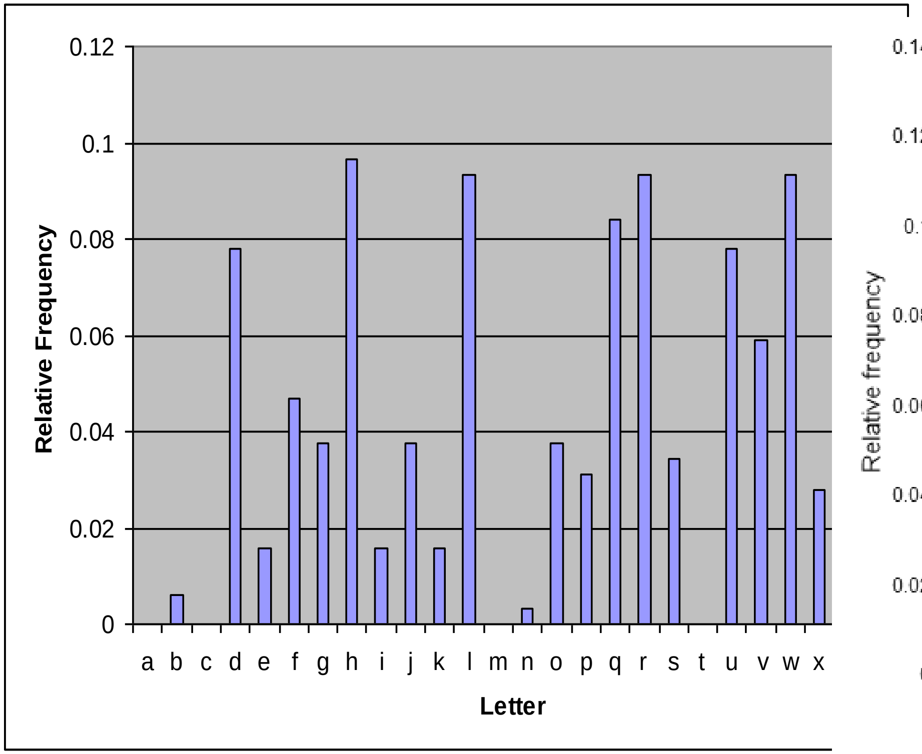
Letter Frequency Analysis

- This is the letter frequency for English
- The most common letter is ‘e’ by a large margin, followed by ‘t’, ‘a’, and ‘o’
- ‘J’, ‘q’, ‘x’, and ‘z’ hardly occur at all

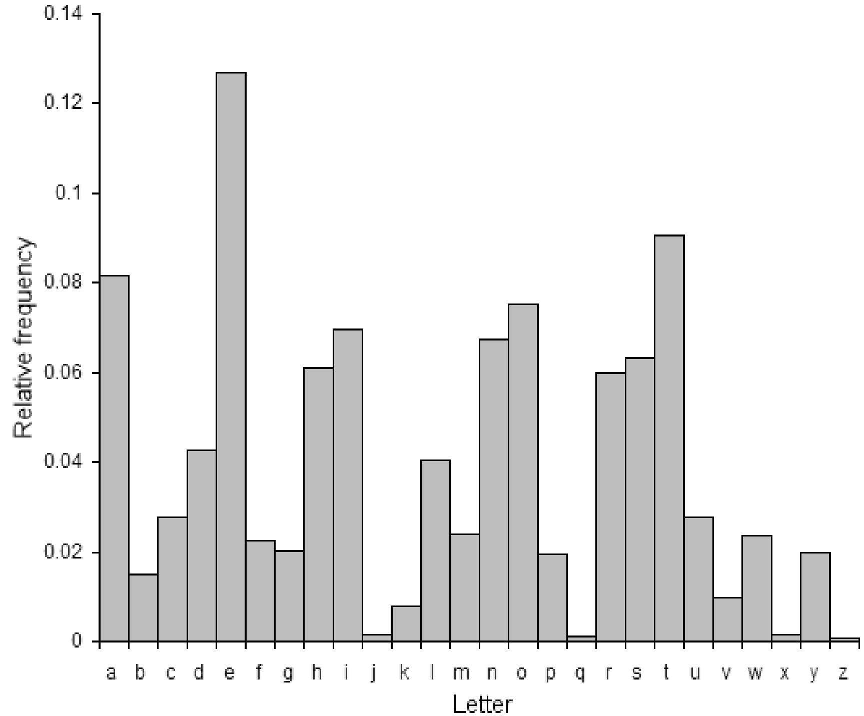


Frequency Analysis in Practice

Ciphertext distribution



English distribution



In this ciphertext we have one letter that occurs more often than any other (h), and 6 that occur a more than any others (d, l, q, r, u, and w)

There is a good chance that h corresponds to e, and d, l, q, r, u, and w correspond to the 6 next most common English letters

Affine Cipher

Let's complicate the encryption function a little bit

$K = Z_{26} \times Z_{26}$ (tentatively)

$Y = e_k(x) = (ax + b) \mod 26$, where $k=(a,b)$

How do you decrypt?

Given a,b, and y, can we find x in Z_{26} such that
$(ax+b) = y \pmod{26}$?

Affine Cipher, Formally

- $P = C$ in Z_{26}
- $K = \{ (a,b) \mid a,b \text{ in } Z_{26}, \ \gcd(a,26)=1 \}$
- $y = e_{(a,b)}(x) = ax + b \pmod{26}$
- $d_{(a,b)}(y) = ?$

What is the size of the keyspace?

Cryptanalysis of Substitution Cipher

Example:

Shift cipher, affine cipher

$P = Z_{26}$ $C = Z_{26}$

K = all possible permutations of Z_{26}

A permutation P is a bijection from $Z_{26} \to Z_{26}$

$e_k(x) = k(x)$

$d_k(x) = k^{-1}(x)$

Statistical cryptanalysis

Ciphertext only attack

plaintext is English letters

Goal of the attacker:

determine the substitution

Idea: Use statistical properties

of English text

Polyalphabetic Ciphers

Previous ciphers were monoalphabetic

- Each alphabetic character mapped to a unique alphabetic character
- This makes statistical analysis easier

Obvious idea: Polyalphabetic ciphers

- Encrypt multiple characters at a time

Poly alphabetic Cipher
Vigenère Cipher

Let m be a positive integer (the key length)

$K = Z_{26} \times .. \times Z_{26} = (Z_{26})^m$

For $k = (k_1, .., k_m)$:

$e_k(x_1, .., x_m) = (x_1 + k_1 \pmod{26}), .., x_m + k_m \pmod{m}))$

$d_k(y_1, .., y_m) = (y_1 - k_1 \pmod{26}), .., y_m - k_m \pmod{m}))$

k = C R Y P T O C R Y P T O C R Y P T

(+ mod 26)

m = W H A T A N I C E D A Y T O D A Y

c = Z Z Z J U C L U D T U N W G C Q S

Security of Vigenere

- Vigenere masks the frequency with which a character appears in a language:
  - one letter in the ciphertext corresponds to multiple letters in the plaintext.
  - Makes the use of frequency analysis more difficult.
- Any message encrypted by a Vigenere cipher is a collection of as many shift ciphers as there are letters in the key.
- Cryptanalysis
  - Find the length of the key.
  - Divide the message into that many shift cipher encryptions.
  - Use frequency analysis to solve the resulting shift ciphers
-

Cryptanalysis of Vigenère Cipher

Thought to thwart statistical analysis until mid-1800

Main idea: first figure out key length (m)

Two identical segments of plaintext are encrypted to the same ciphertext if they are δ position apart,

where $\delta = 0 \pmod m$

Kasiski Test:

find all identical segments of length > 3 and record the distance between them: $\delta_1, \delta_2, \ldots$

M divides $\gcd(\delta_1, \delta_2), \ldots$

- Thanks