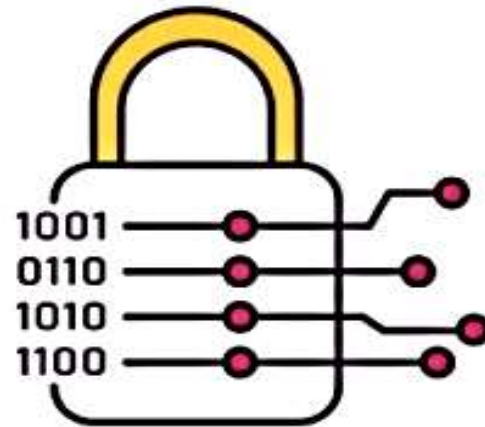


Information Security

CS3002

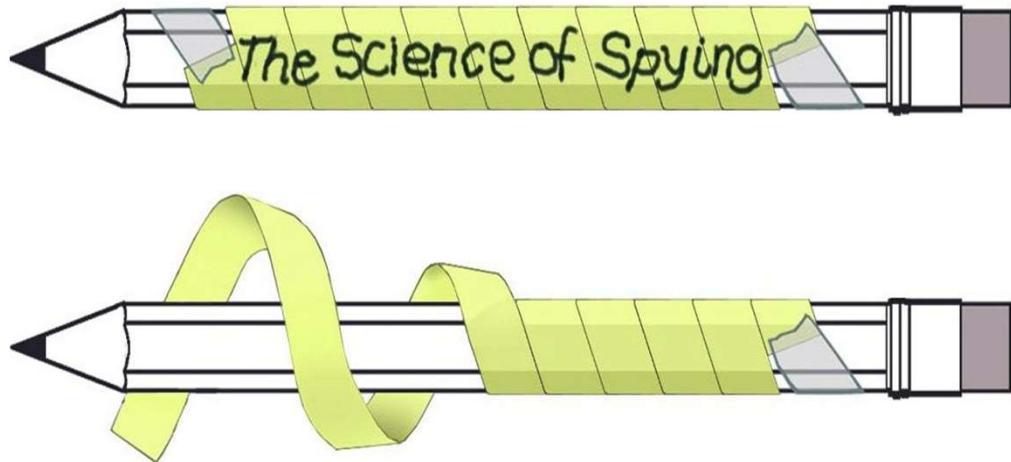
Lecture 3
26th August 2024

Dr. Rana Asif Rehman
Email: r.asif@lhr.nu.edu.pk



Cryptography

Old Cryptography Methods



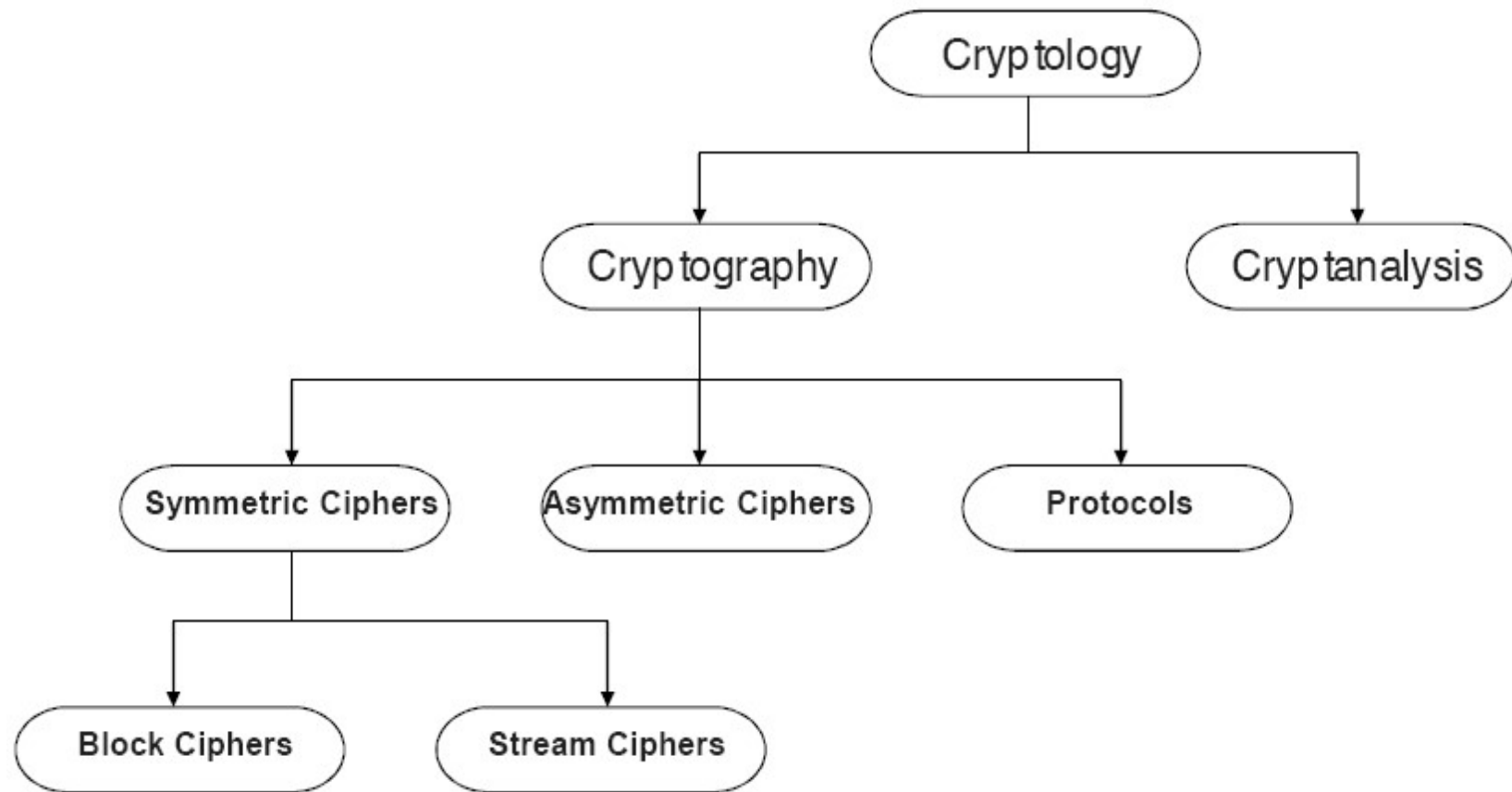
Some Basic Terminology

- **Plaintext** - original message
- **Ciphertext** - coded message
- **Encryption algorithm** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext

Some Basic Terminology (cont.)

- **Decryption algorithm** - algorithm for transforming ciphertext to plaintext
- **DeCipher** – converting ciphertext to plaintext .
- **Cryptography** - Study Of Encryption Principles/Methods
- **Cryptanalysis (Codebreaking)** - Study Of Principles/ Methods Of Deciphering Ciphertext *Without* Knowing Key
- **Cryptology** - Field of Both Cryptography And Cryptanalysis

Classification of the Field of Cryptology



Adopted with thanks from: Chapter 1 of Understanding Cryptography by Christof Paar and Jan Pelzl

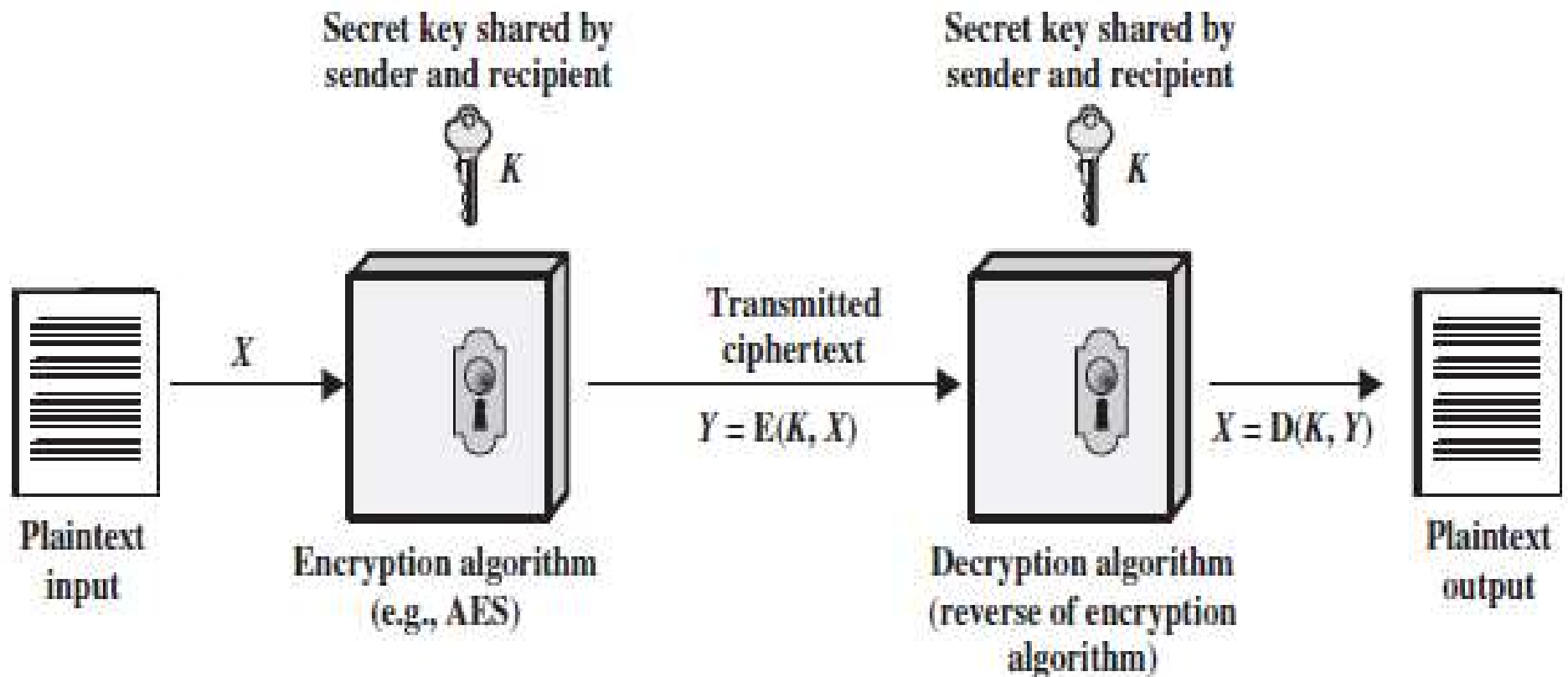


Symmetric Cryptography

Symmetric Encryption

- Or conventional / private-key / single-key
- Sender and recipient share a common key
- All classical encryption algorithms are private-key
- Was only type prior to invention of public-key in 1970's
- And by far most widely used

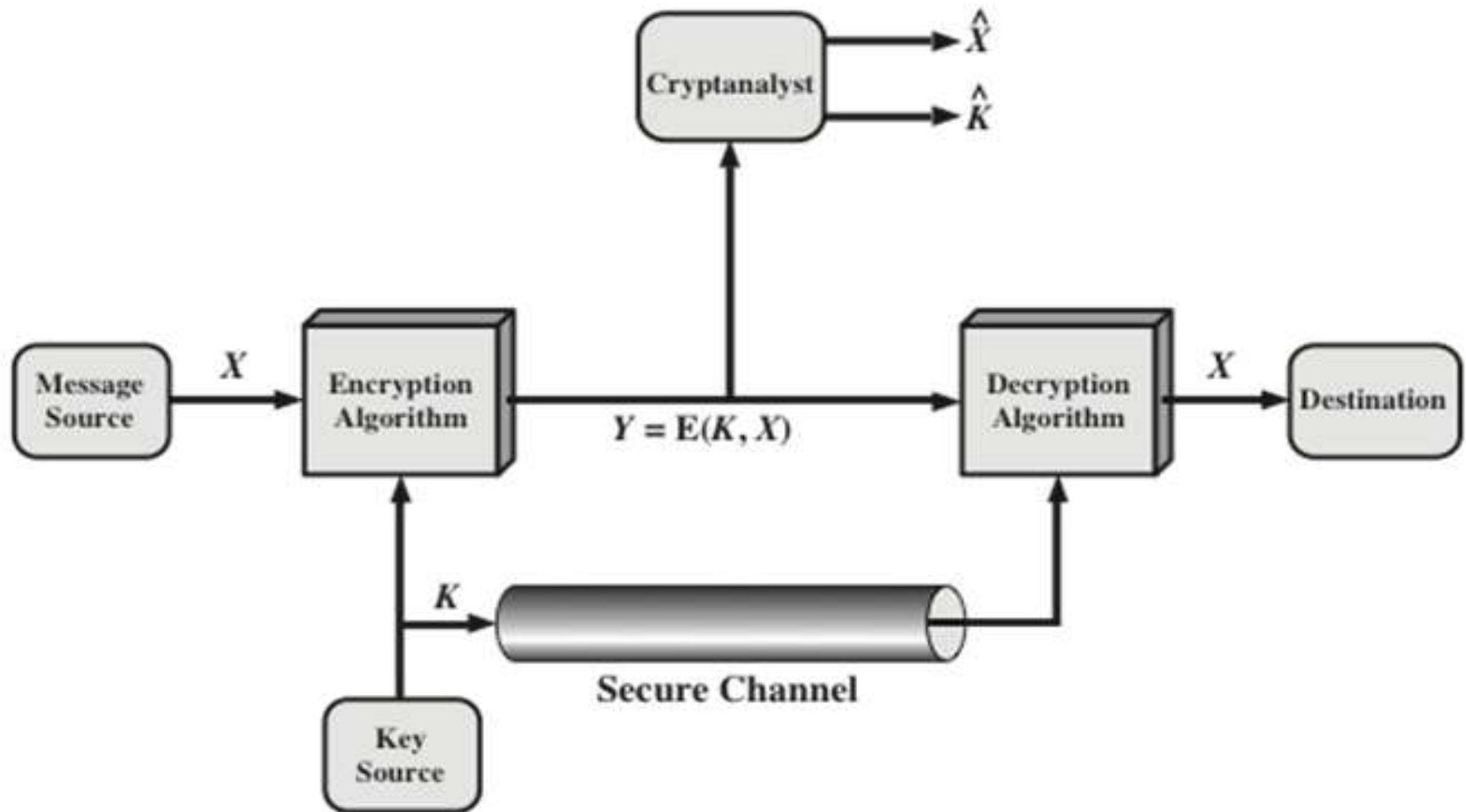
Simplified Model of Symmetric Encryption



Requirements

- Two requirements for secure use of symmetric encryption:
 - A strong encryption algorithm
 - The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
 - A secret key known only to sender / receiver
 - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

Model of Symmetric Cryptosystem



Model of Symmetric Cryptosystem (cont.)

With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext $Y = [Y_1, Y_2, \dots, Y_N]$. We can write this as

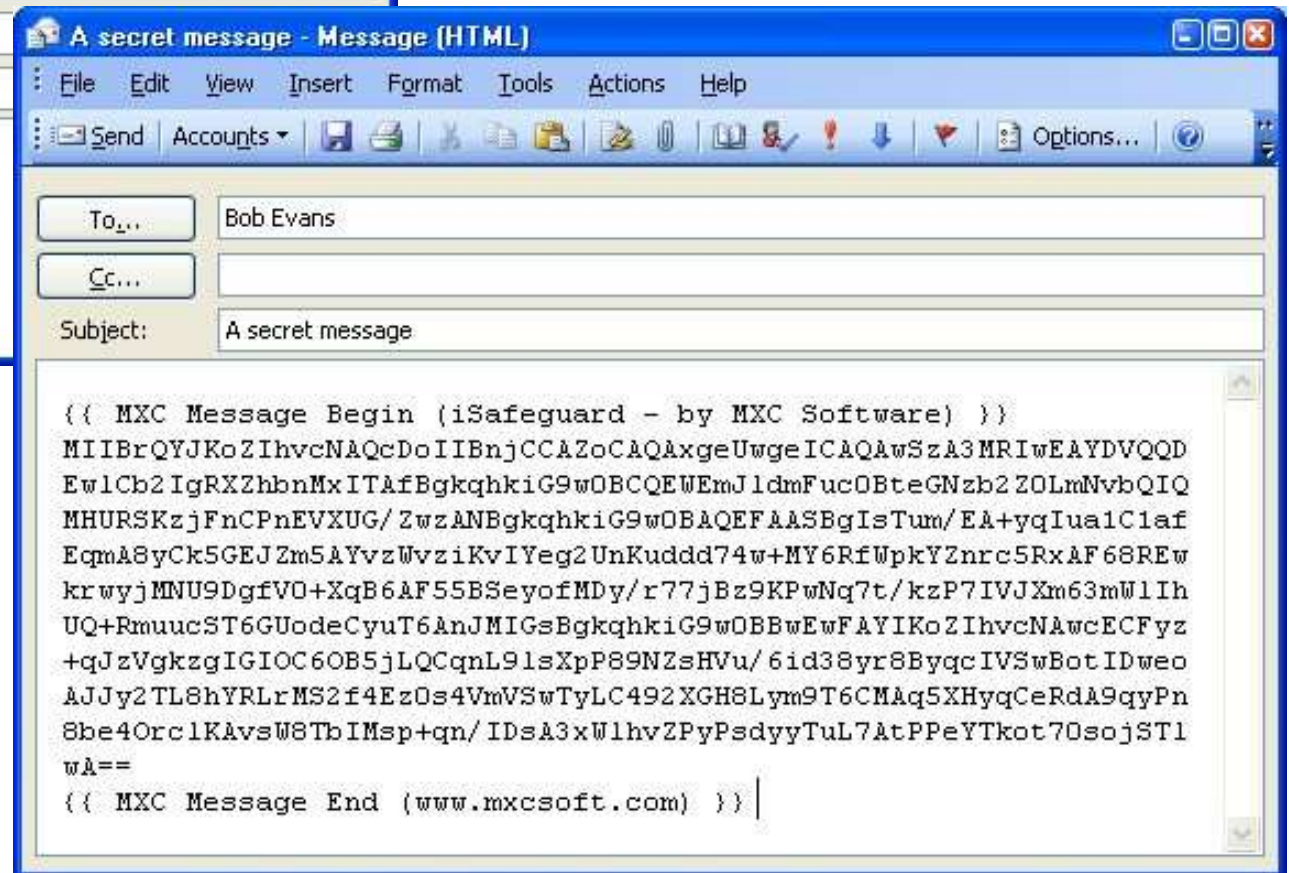
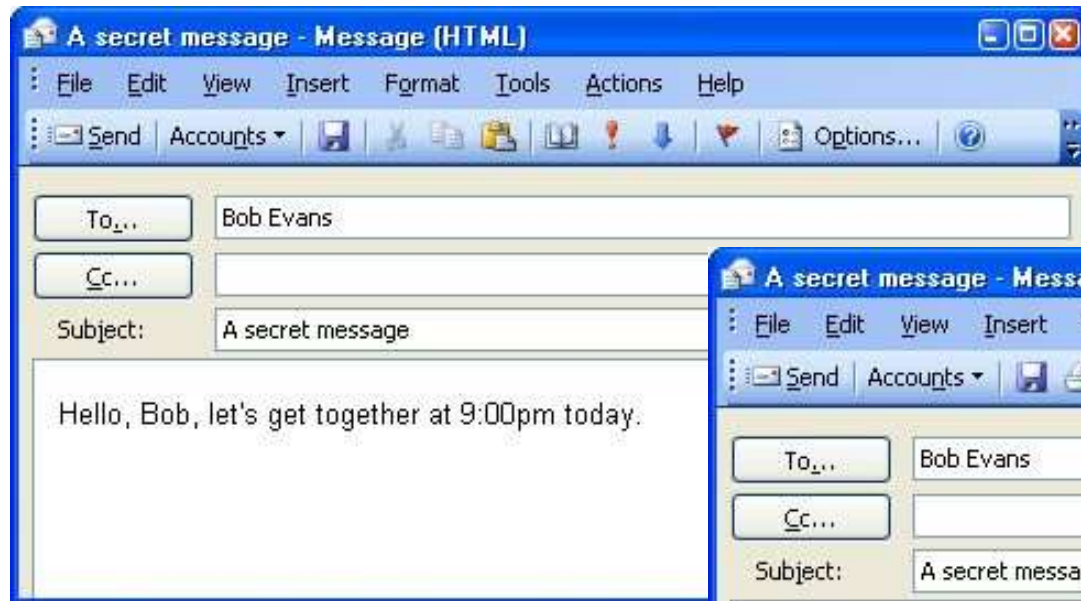
$$Y = E(K, X)$$

The intended receiver, in possession of the key, is able to invert the transformation:

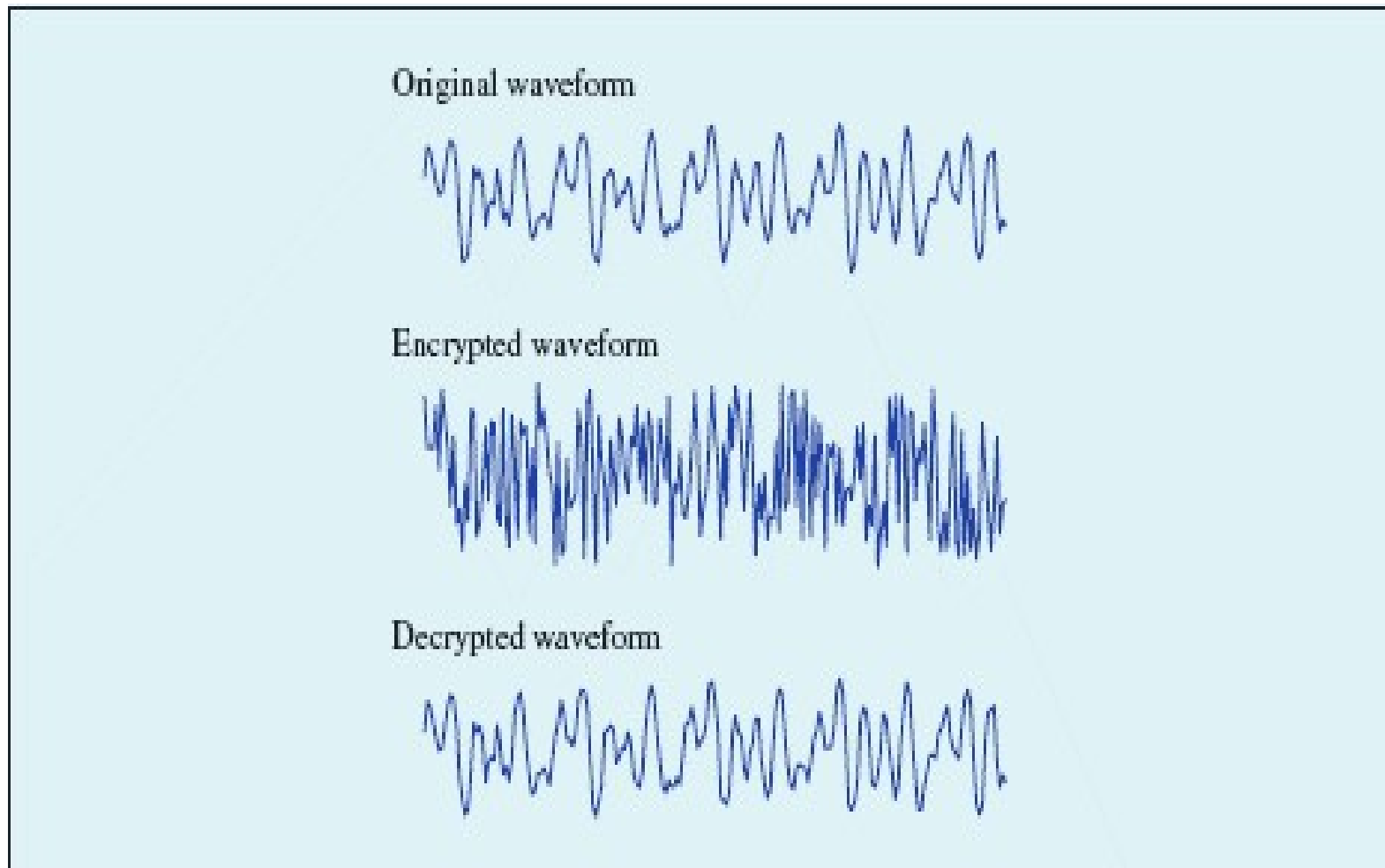
$$X = D(K, Y)$$

An opponent, observing Y but not having access to K or X , may attempt to recover X or K or both X and K .

Cryptographic Message



Cryptographic Speech Signal



Cryptographic Image



Original image

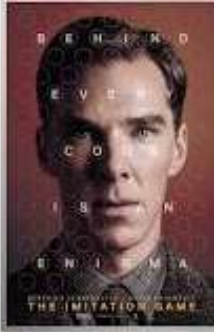


Modes other than ECB result in pseudo-randomness

Turing's work during the Second World War was so crucial that Winston Churchill acknowledged his role, saying that Turing made the single biggest contribution to Allied victory.

The Imitation Game

2014 · Drama/Thriller · 1h 54m




8/10
IMDb

91%
Rotten Tomatoes

92% liked this film

Google users



In 1939, newly created British intelligence agency MI6 recruits Cambridge mathematics alumnus Alan Turing (Benedict Cumberbatch) to crack Nazi codes, including Enigma – which cryptanalysts had thought unbreakable. Turing's team, including Joan Clarke (Keira Knightley), analyze Enigma messages while he builds a machine to decipher them. Turing and team finally succeed and become heroes, but in 1952, the quiet genius encounters disgrace when authorities reveal he is gay and send him to prison.

Initial release: 7 January 2015 (Egypt)

Director: Morten Tyldum

Box office: 233.6 million USD

Awards: Academy Award for Best Writing Adapted Screenplay, [MORE](#) ▼

Nominations: Academy Award for Best Picture, [MORE](#) ▼



<http://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code>

Classical Symmetric Ciphers

- Where letters of plaintext are replaced by other letters or by numbers or symbols.
- Or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.



Classical Symmetric Ciphers

- Classical Substitution Ciphers
- Classical Transposition Ciphers



Classical Symmetric Ciphers

- Classical Substitution Ciphers
 - Caesar Cipher
 - Monoalphabetic Cipher
 - Vigenere Cipher
 - One-Time Pad

1. Caesar Cipher

- Earliest known substitution cipher.
 - The Roman emperor Julius Caesar used in his diplomatic communications
- First attested use in military affairs.
- Replaces each letter by 3rd letter on
- Example:

meet me after the toga party
phhw ph diwhu wkh wrjd sduwb



Caesar Cipher (cont.)

- Can define transformation as:

plain: 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
cipher: 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

- Then have caesar cipher as:

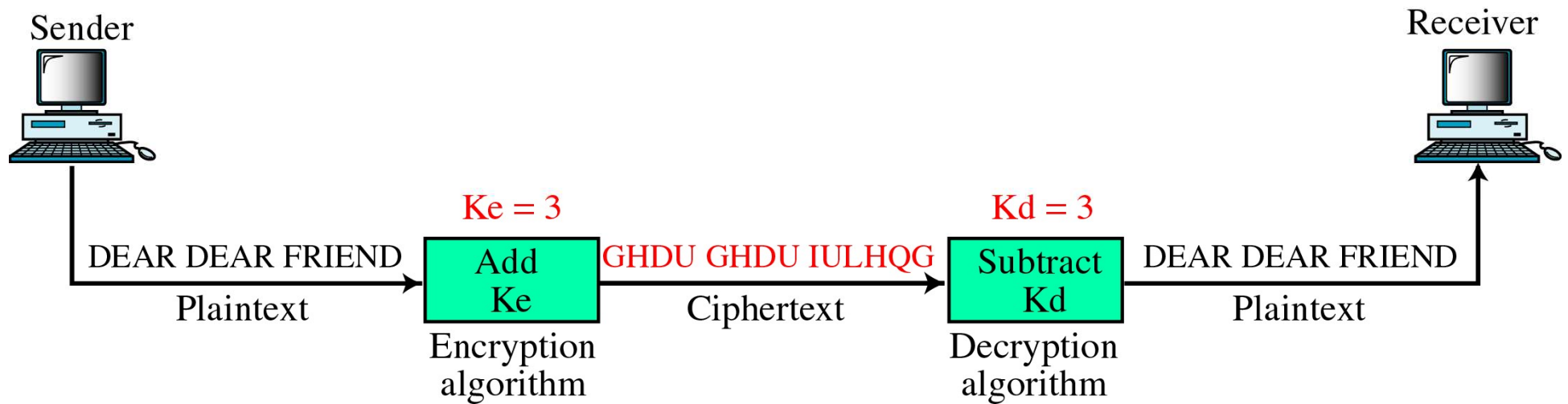
a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

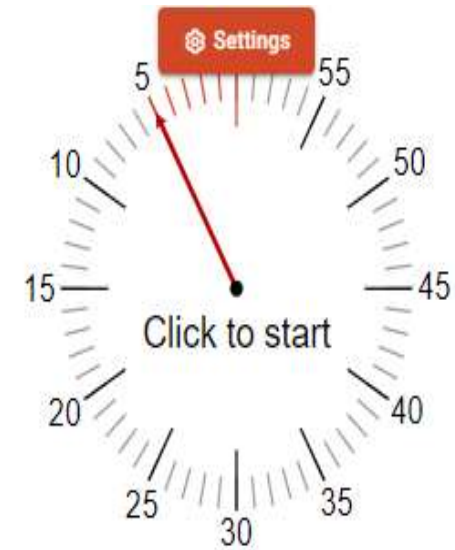
$$c = E(k, p) = (p + k) \bmod (26)$$

$$p = D(k, c) = (c - k) \bmod (26)$$

Caesar Cipher (cont.)



Activity Time



Plaintext: **LETS TAKE A TEN MINUTES BREAK**

Ciphertext: **OHVV WDNH D WHQ PLQXWHV EUHDN**

Cryptanalysis of Caesar Cipher

- Only have 25 possible Keys
 - A maps to B,C,..Z
- Could simply try each in turn
- **A brute force search**
 1. The encryption and decryption algorithms are known.
 2. There are only 25 keys to try.
 3. The language of the plaintext is known and easily recognizable.
 - e.g. Break ciphertext "GCUA VQ DTGCM"

KEY		PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1		oggv	og	chvgt	vjg	vqic	retva
2		nffu	nf	bgufs	uif	uphb	qbsuz
3		meet	me	after	the	toga	party
4		ldds	ld	zesdq	sgd	snfz	ozqsx
5		kccr	kc	ydrpc	rfe	rmey	nyprw
6		jbbq	jb	xcqbo	qeb	qldx	mxoqv
7		iaap	ia	wbpan	pda	pkcw	lwnpu
8		hzzo	hz	vaozm	ocz	ojbv	kvmot
9		gyyn	gy	uznyl	nby	niau	julns
10		fxxm	fx	tymxk	max	mhzt	itkmr
11		ewwl	ew	sxlwj	lzw	lgys	hsjlq
12		dvvk	dv	rwkvi	kyv	kfxr	grikp
13		cuuu	cu	qvjuh	jxu	jewq	fqhjo
14		btti	bt	puitg	iwt	idvp	epgin
15		assh	as	othsf	hvs	hcuo	dofhm
16		zrrg	zr	nsgrc	gur	gbtn	cnegl
17		yqqf	yq	mrfqd	ftq	fasm	bmdfk
18		xppe	xp	lqepc	esp	ezrl	alcej
19		wood	wo	kpdob	dro	dyqk	zkbdi
20		vnnc	vn	jocna	cqn	cxpj	yjach
21		ummb	um	inbmz	bpm	bwoi	xizbg
22		tlla	tl	hmaly	aol	avnh	whyaf
23		skkz	sk	qlzkk	znk	zumg	vgxze
24		rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25		qiix	qi	ejxiv	xli	xske	tevxc

Brute Force Feasibility

- In most networking situations, we can assume that the algorithms are known.
- What generally makes brute-force cryptanalysis impractical is the use of an algorithm that employs a large number of keys.
 - For example, the triple DES algorithm makes use of a 168-bit key, giving a key space of 2^{168} or greater than $3.7 * 10^{50}$ possible keys.

2. Monoalphabetic Cipher

- With only 25 possible keys, the Caesar cipher is far from secure.
- Rather than just shifting the alphabet could shuffle (jumble) the letters **arbitrarily [permutation]**
- Each plaintext letter maps to a different random ciphertext letter
- Hence key is 26 letters long

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: IFWEWISHTOREPLACELETTERS

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

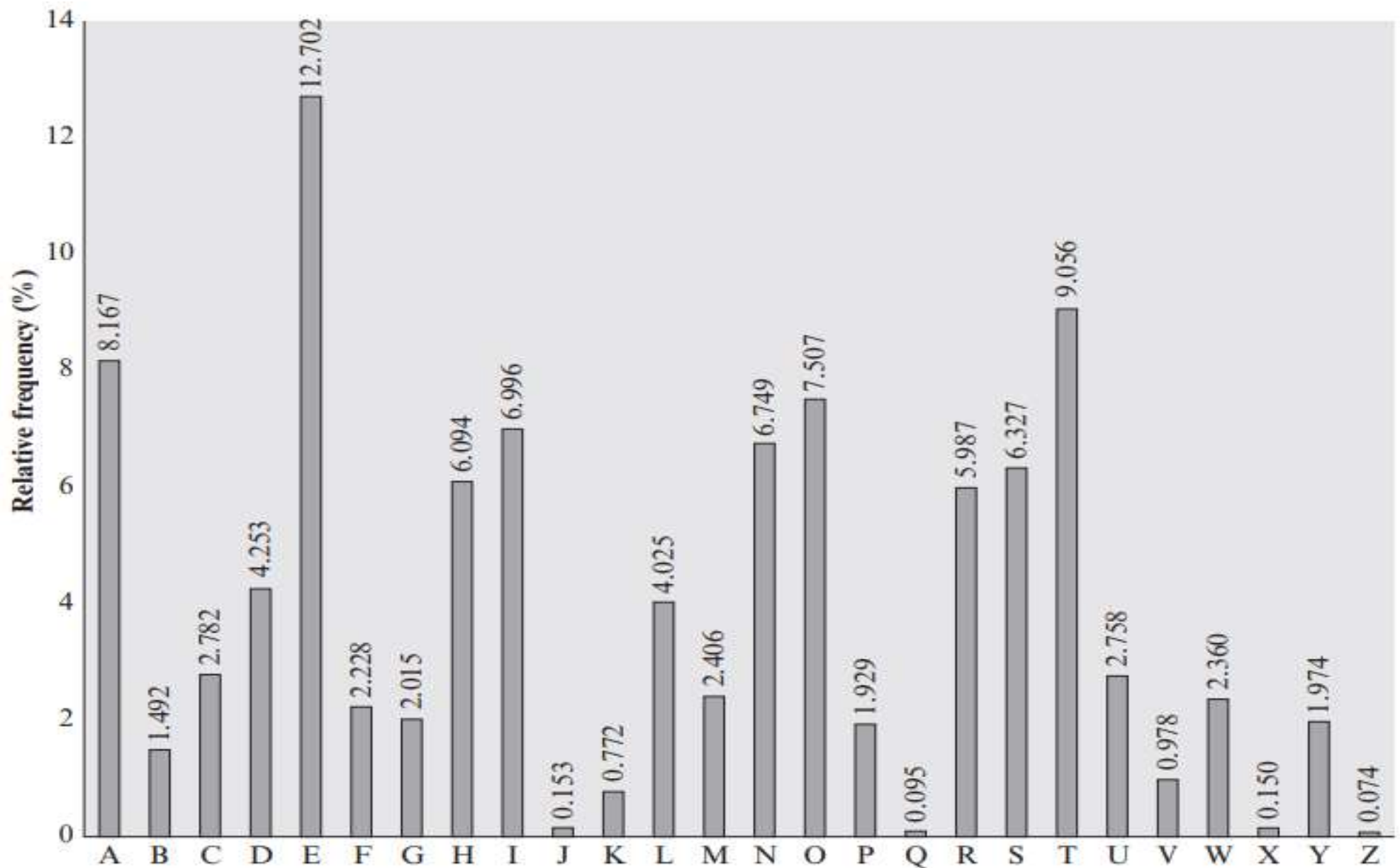
Monoalphabetic Cipher Security

- Now have a total of $26! = 4 \times 10^{26}$ keys
- With so many keys, might think is secure
- But would be **!!!WRONG!!!**
- Problem is language characteristics

Language Redundancy and Cryptanalysis

- Human languages are **redundant** e.g. "Th lrd s m shphrd shll nt wnt" letters are not equally commonly used.
- In English E is by far the most common letter
 - Followed by T,R,N,I,O,A,S
- Other letters like Z,J,K,Q,X are fairly rare
- Have tables of single, double & triple letter frequencies for various languages

English Letter Frequencies



Use in Cryptanalysis

- Key concept - monoalphabetic substitution ciphers do not change relative letter frequencies.
- Calculate letter frequencies for ciphertext.
- Compare counts/plots against known values.
- For monoalphabetic must identify each letter
 - tables of common double/triple letters help

Language Redundancy and Cryptanalysis

- Cipher Text

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

Example Cryptanalysis

- given cipher text:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAI Z
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- count relative letter frequencies
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the

So far, then, we have

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAI Z
t a e e te a that e e a a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
e t ta t ha e ee a e th t a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
e e e tat e the t

Example Cryptanalysis (cont.)

- Proceeding with trial and error finally get:

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow