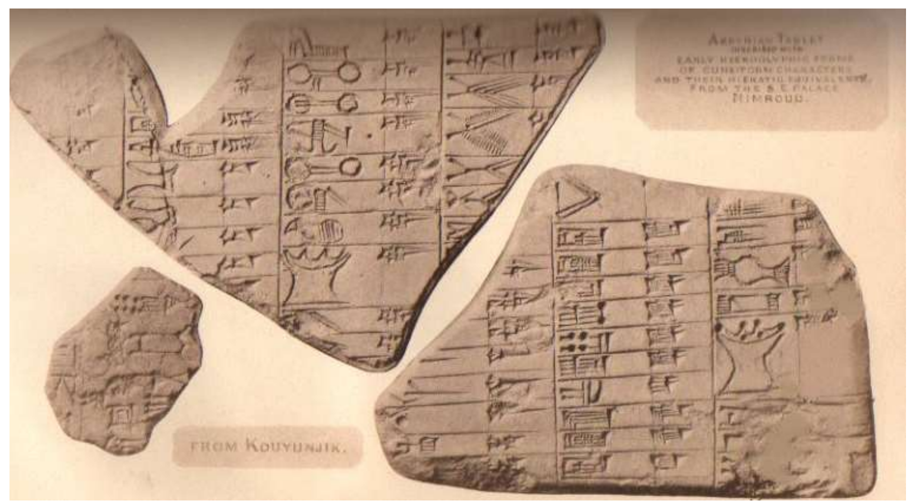
Cryptography

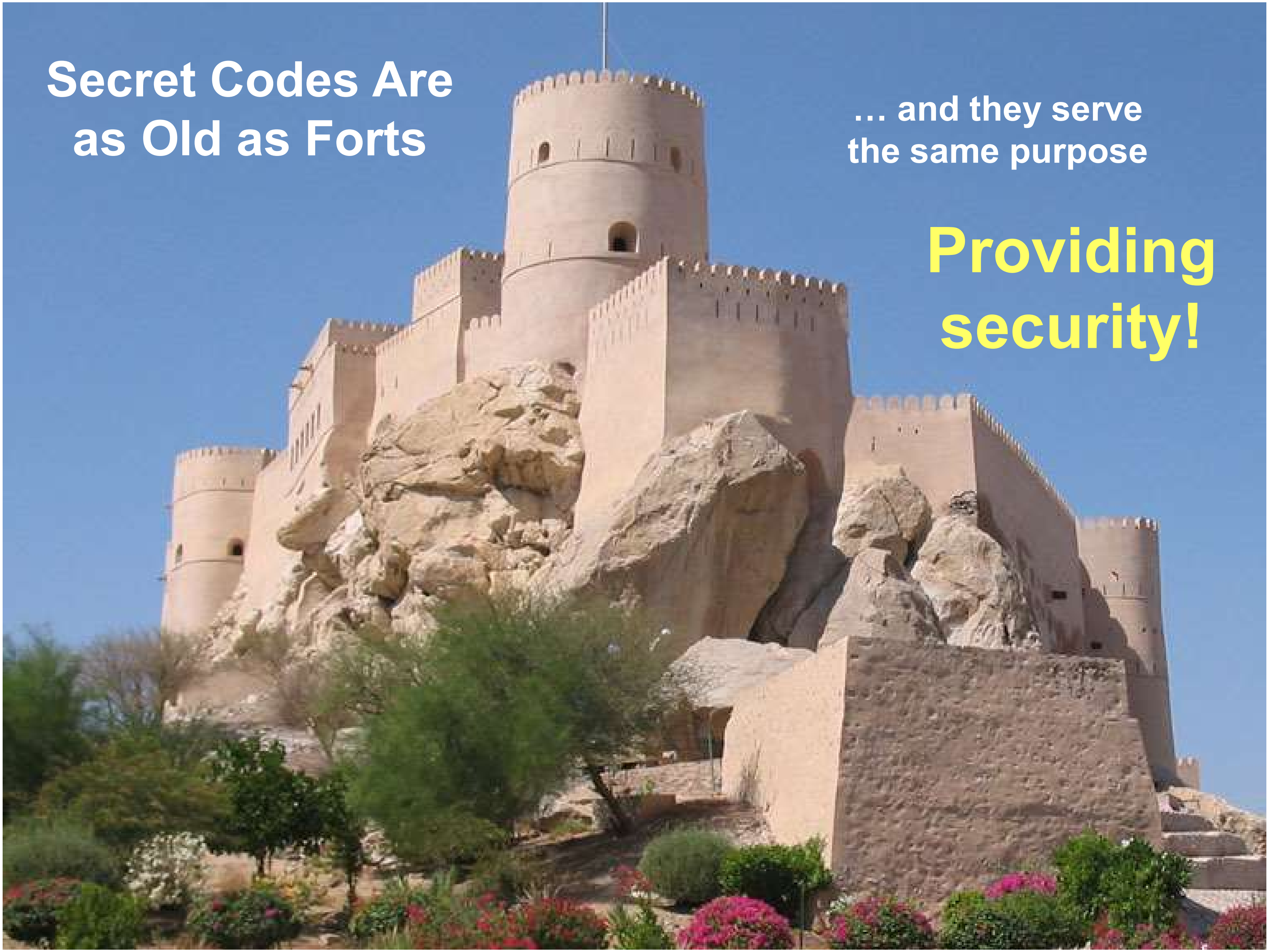
A Lecture in CE Freshman Seminar Series:
Ten Puzzling Problems in Computer Engineering

About This Presentation

Edition	Released	Revised	Revised	Revised	Revised
First	Apr. 2007	Apr. 2008	Apr. 2009	Apr. 2010	Apr. 2011
		Apr. 2012	Apr. 2015	Apr. 2016	Apr. 2020

Puzzles and Cryptograms in Archeology




Secret Codes Are as Old as Forts
… and they serve the same purpose
Providing security!

Some Simple Cryptograms

Cipher: YHPARGOTPYRC OT EMOCLEW
Plain: WELCOME TO CRYPTOGRAPHY

Cipher: EHT YPS WSI RAE GNI LBA CEU TAO
Plain: THE SPY ISW EAR ING ABL UEC OAT

Cipher: ICCRAANCTKBEEDLTIHEIVSECYOODUE
Plain: I C A N T B E L I E V E Y O U
C R A C K E D T H I S C O D E

	1	2	3	4	5	6	7	8
Cipher:	SSA	PSE	TJX	SME	CRE	STO	THI	GEI
Plain:	THI	SME	SSA	GEI	STO	PSE	CRE	TJX
Key:	7	4	1	8	6	2	5	3

Cipher: AMY TAN'S TWINS ARE CUTE KIDS
Plain: A T T A C K

Simple Substitution Ciphers

Decipher the following text, which is a quotation from a famous scientist.
Clue: Z stands for E

"CEBA YUC YXSENM PDZ SERSESYZ, YXZ QESOZDMZ PEJ XQKPE MYQGSJSYA, PEJ S'K ECY MQDZ PLCQY YXZ RCDKZD."
PBLZDY ZSEMYZSE

"CEBA YUC YXSENM PDZ SERSESYZ, YXZ QESOZDMZ PEJ XQKPE
"ONLY TWO THINGS ARE INFINITE, THE UNIVERSE AND HUMAN

MYQGSJSYA, PEJ S'K ECY MQDZ PLCQY YXZ RCDKZD."
STUPIDITY, AND I'M NOT SURE ABOUT THE FORMER."

PBLZDY ZSEMYZSE
ALBERT EINSTEIN

X stands for **H**?

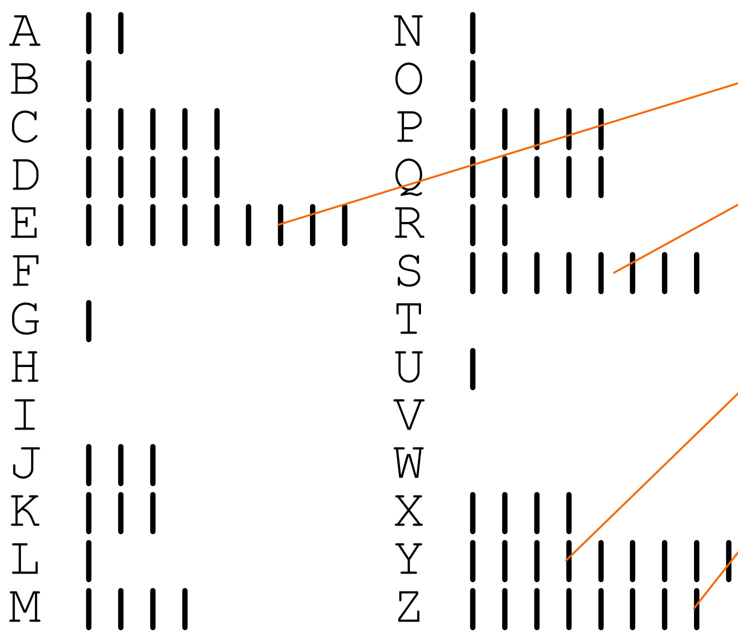
Contextual information facilitated the deciphering of this example

Breaking Substitution Ciphers

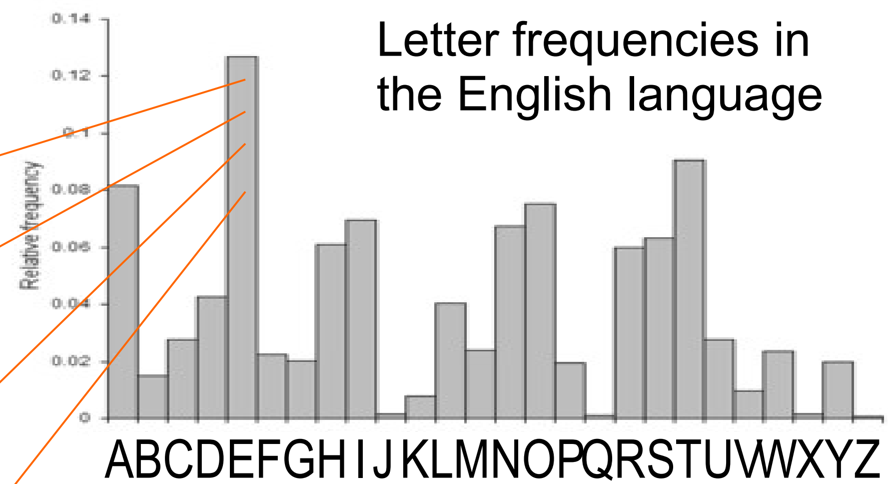
The previous puzzle, with punctuation and other give-aways removed:

CEBA YUC YXSENM PDZ SERSESYZ YXZ QESOZDMZ PEJ XQKPE MYQGSJSYA PEJ SK ECY MQDZ PLCQY YXZ RCDKZD

Letter frequencies in the cipher:



Letter frequencies in the English language



Most frequently used 3-letter words:

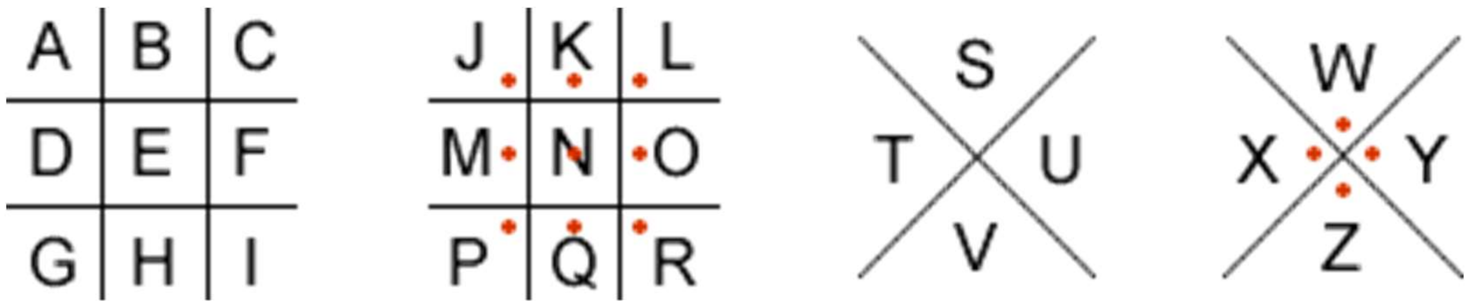
THE AND FOR WAS HIS

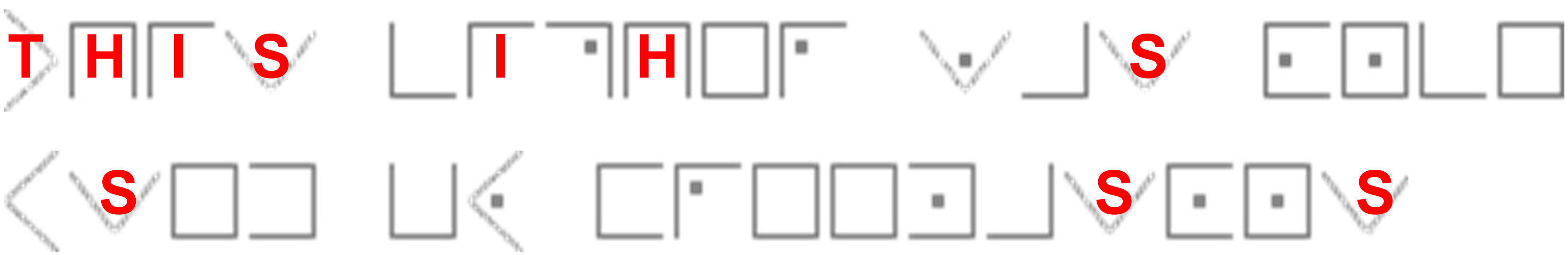
Most frequently used letter pairings:

TH HE AN IN ER ON RE ED

The Pigpen Cipher

Encoded message:





This is a substitution cipher, with all the weaknesses of such ciphers

Q1: Write the message above in the cipher used for the quote on Slide 6.

The Code of Emojis

Q2: Decode at least four of the following movie titles written in emojis.

Run in papers of Friday, Oct. 13, 2006

CELEBRITY CIPHER

by Luis Campos

Celebrity Cipher cryptograms are created from quotations by famous people, past and present.
Each letter in the cipher stands for another.

Today's clue: O equals J

" X P Z T F Y B A T H X T R T Y K M Y

M G V Y K X G E J M Z A T Y Y T L Y K M G

G B Y K X G E . G B J X W G B J Y K M Y

Z B U T Y X U T Z G B Y K X G E X Z A T Y Y T L . "

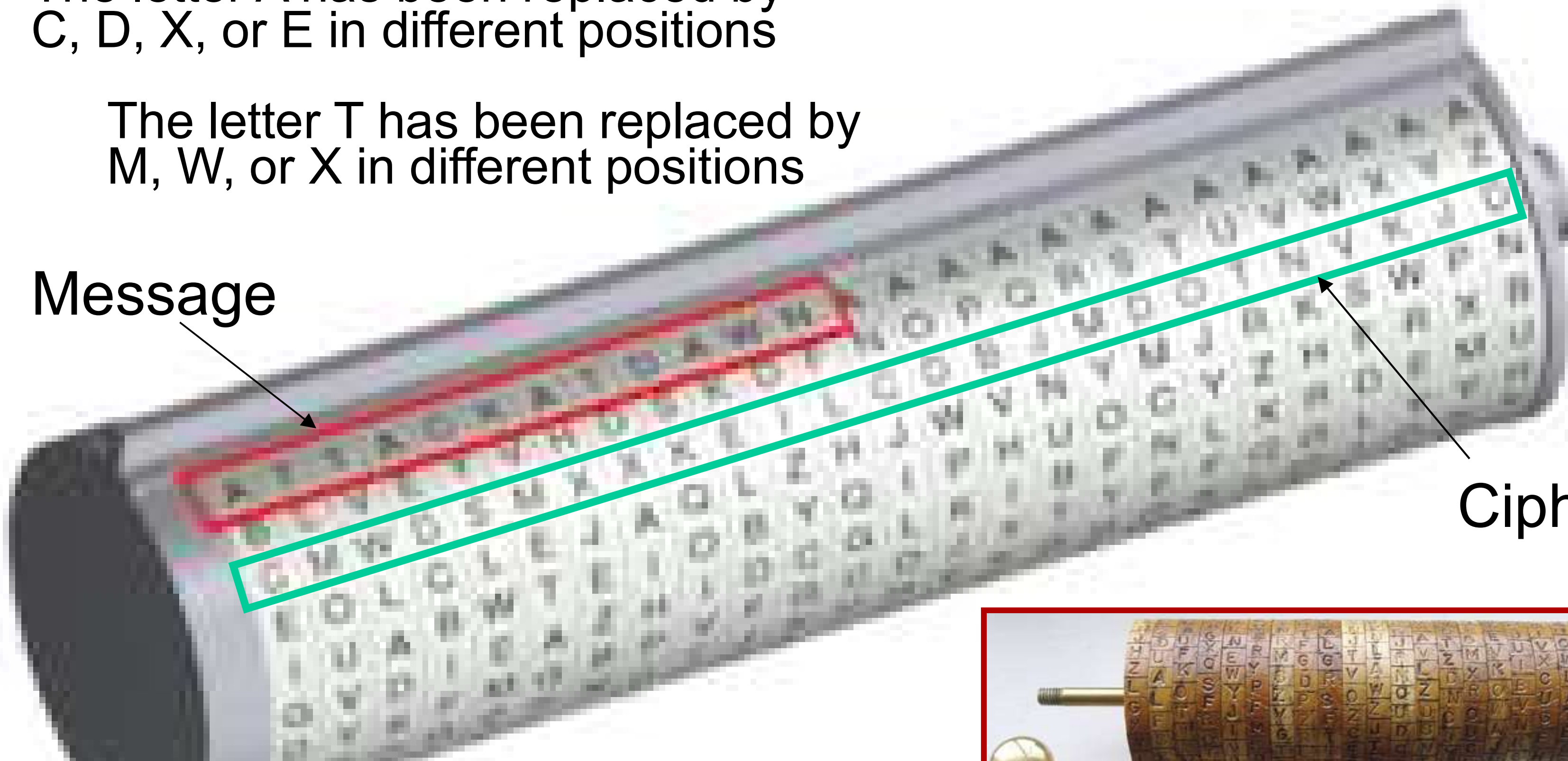
– E H T G F M O M S W Z B G

PREVIOUS SOLUTION — "Art for the sake of truth, for the sake of what is beautiful and good – that is the creed I seek." – George Sand

More Sophisticated Substitution Ciphers

The letter A has been replaced by
C, D, X, or E in different positions

The letter T has been replaced by
M, W, or X in different positions

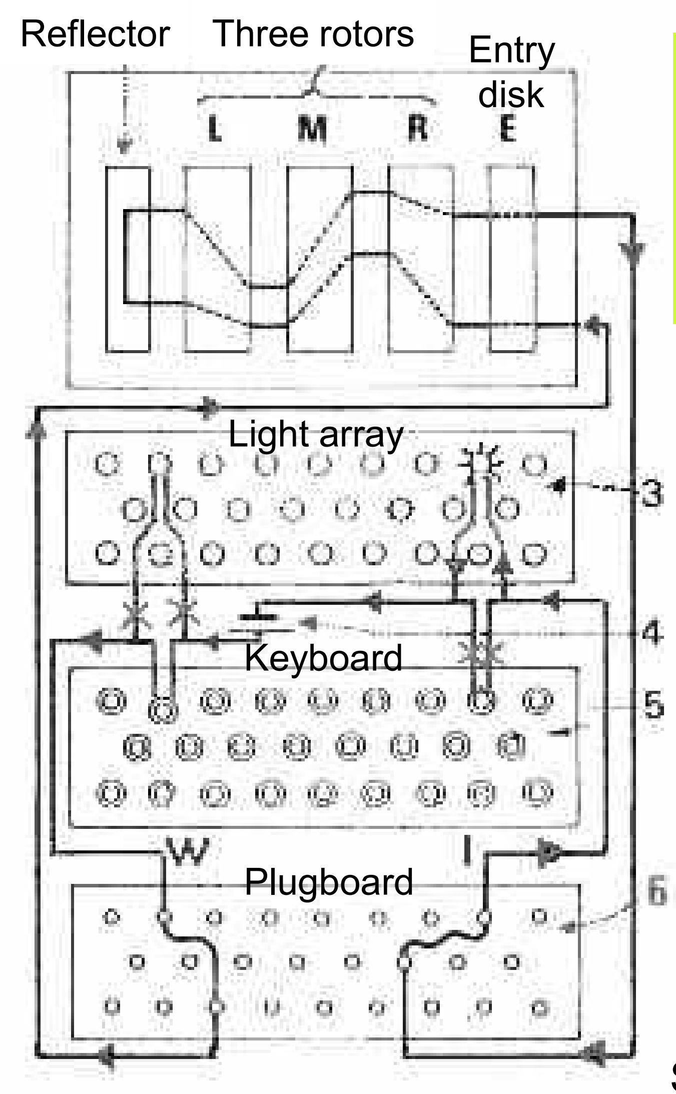


Message

Cipher

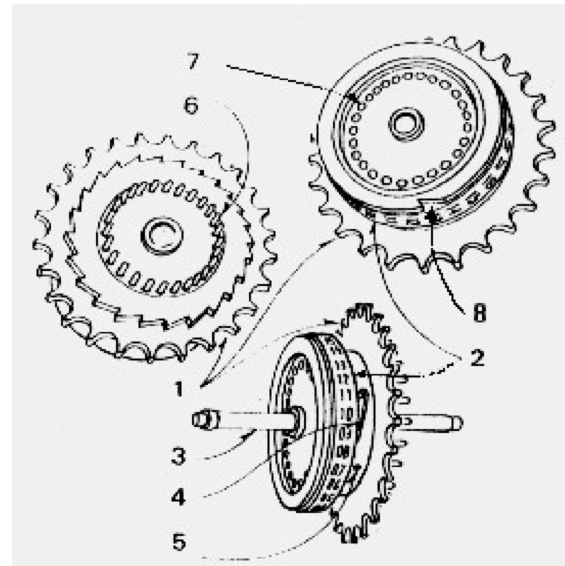
25 rotating wheels

The German Enigma Encryption Machine



(4) Connection goes through the 3 rotors, is “reflected”, returns through the 3 rotors, leads to plugboard

(5) Eventually, the “I” light is illuminated



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

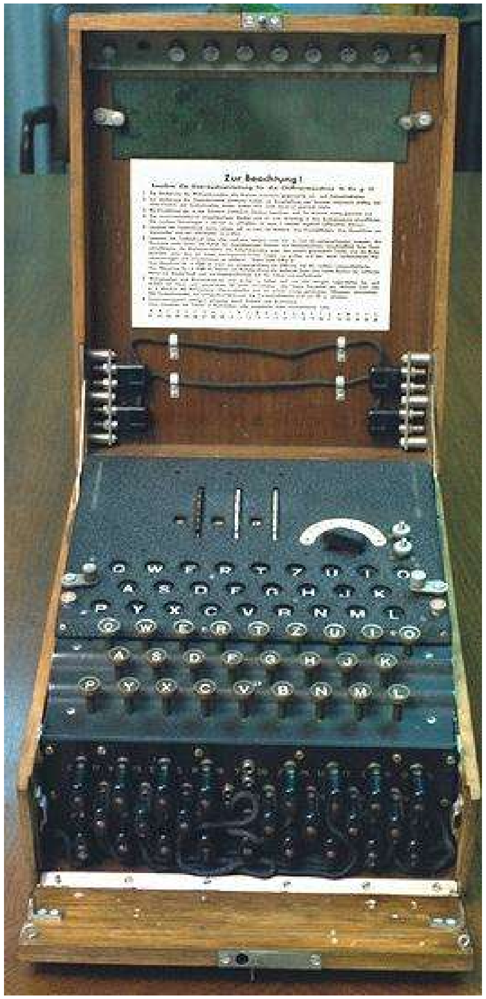
(2) Battery now connected to W on plugboard . . .

(1) W pressed on keyboard

(3) . . . which is wired to X plug

Source: http://www.codesandciphers.org.uk/enigma/index.htm

Alan Turing and the Enigma Project



The German Enigma encryption machine

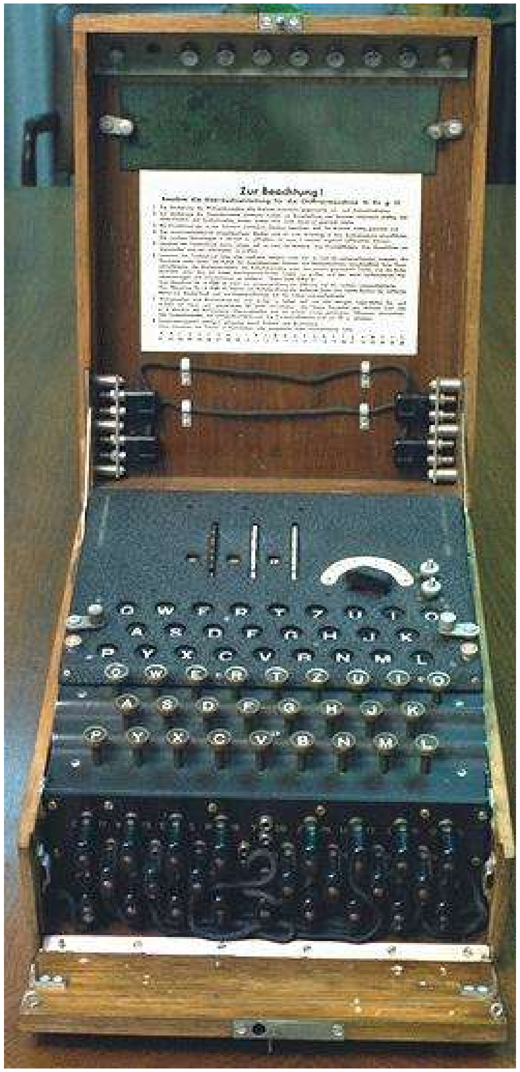
Alan M. Turing
1912-1954

The Mansion at Bletchley Park
(England's wartime codebreaking center)

Enigma's rotor assembly

Source: http://www.ellsbury.com/enigmabombe.htm

More on the Enigma and the Turing Biopic



Brief demo of Enigma (London Science Museum)
https://youtu.be/TYX691q2J2c

How accurate is “The Imitation Game” biopic?
http://www.slate.com/blogs/browbeat/2014/12/03/the_imitation_game_fact_vs_fiction_how_true_the_new_movie_is_to_alan_turing.html

Q3: Write a short paragraph about how the allies managed to break the Enigma code.

A Simple Key-Based 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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Agreed upon secret key: **ourkey**

Plain text:	A	T	T	A	C	K	A	T	D	A	W	N
	00	19	19	00	02	10	00	19	03	00	22	13
Secret key:	o	u	r	k	e	y	o	u	r	k	e	y
	14	20	17	10	04	24	14	20	17	10	04	24
Sum:	14	39	36	10	06	34	14	39	20	10	26	37
Modulo 26 sum:	14	13	10	10	06	08	14	13	20	10	00	11
Cipher text:	O	N	K	K	G	I	O	N	U	K	A	L
Secret key:	14	20	17	10	04	24	14	20	17	10	04	24
Difference:	00	-7	-7	00	02	-16	00	-7	03	00	-4	-13
Modulo 26 diff.:	00	19	19	00	02	10	00	19	03	00	22	13
Recovered text:	A	T	T	A	C	K	A	T	D	A	W	N

One can break such key-based ciphers by doing letter frequency analysis with different periods to determine the key length

The longer the message, the more successful this method of attack

Decoding a Key-Based 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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Agreed upon secret key: **freshman**

Cipher text:	B	Y	E	L	P	E	Y	B	Z	I	R	S	T	Q
	01	24	04	11	15	04	24	01	25	08	17	18	19	16
Secret key:	f	r	e	s	h	m	a	n	f	r	e	s	h	m
	05	17	04	18	07	12	00	13	05	17	04	18	07	12
Difference:	-4	07	00	-7	08	-8	24	-12	20	-9	13	00	12	04
Modulo 26 diff.:	22	07	00	19	08	18	24	14	20	17	13	00	12	04
Plain text:	W	H	A	T	I	S	Y	O	U	R	N	A	M	E

Decipher the coded message and provide a reply to it using the same key (ignore blanks)

Reply:	J	O	H	N	S	M	I	T	H
	09	14	07	13	18	12	08	19	07
Secret key:	f	r	e	s	h	m	a	n	f
	05	17	04	18	07	12	00	13	05
Sum:	14	31	11	31	25	24	08	32	12
Modulo 26 sum:	14	05	11	05	25	24	08	06	12
Cipher text:	O	F	L	F	Z	Y	I	G	M

Q4: Show the encoding and decoding of the message "I SENT AN ATTENDANCE REPORT FOR ECE 1B" Using the secret key "MYKEYBASEDCIPHER".

Key-Based Cipher with Binary Messages

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

*	&	#	@	%	$
26	27	28	29	30	31

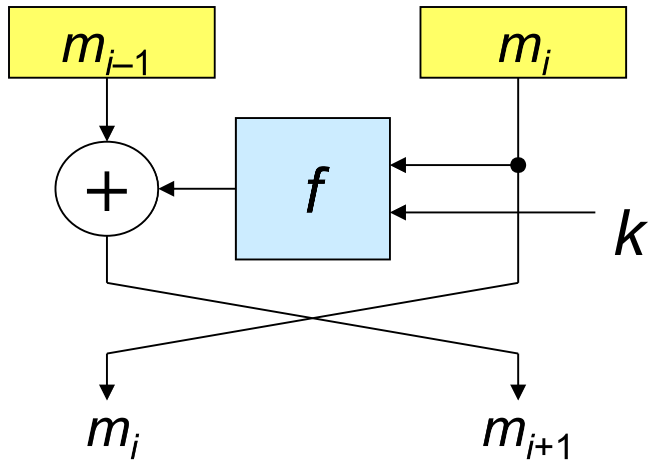
Agreed upon secret key (11 bits): 0 1 0 0 0 1 1 1 0 1 0

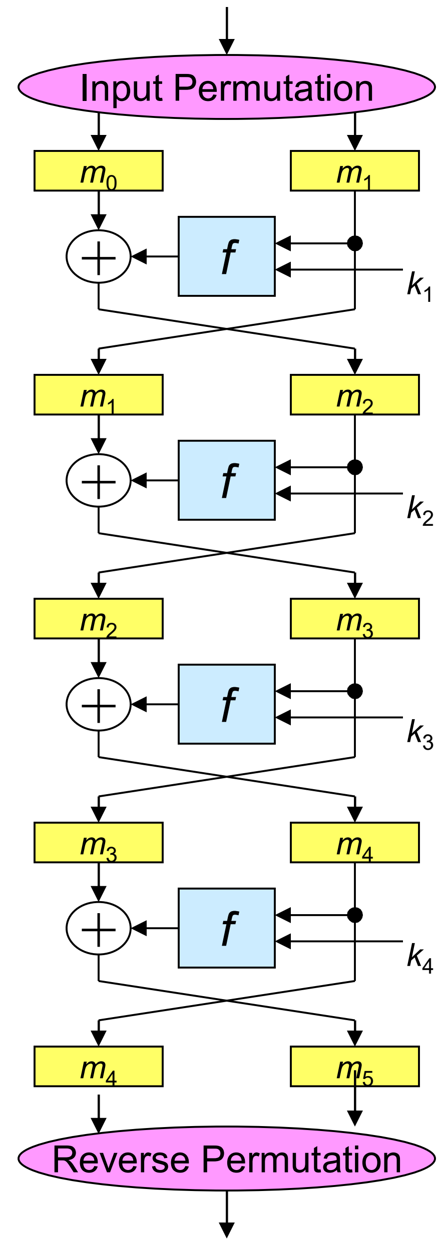
	07 = H	04 = E	24 = Y
Plain text:	0 0 1 1 1	0 0 1 0 0	1 1 0 0 0
Secret key:	0 1 0 0 0	1 1 1 0 1	0 0 1 0 0
XOR: (mod-2 add)	0 1 1 1 1	1 1 0 0 1	1 1 1 0 0
	15 = P	25 = Z	28 = #
Secret key:	0 1 0 0 0	1 1 1 0 1	0 0 1 0 0
XOR:	0 0 1 1 1	0 0 1 0 0	1 1 0 0 0

Symmetric: Encoding and decoding algorithms are the same

Data Encryption Standard (DES)

Feistel block:
The data path is divided into left (m_{i-1}) and right (m_i) halves. A function *f* of m_i and a key k_i is computed and the result is XORed with m_{i-1}. Right and left halves are then interchanged.

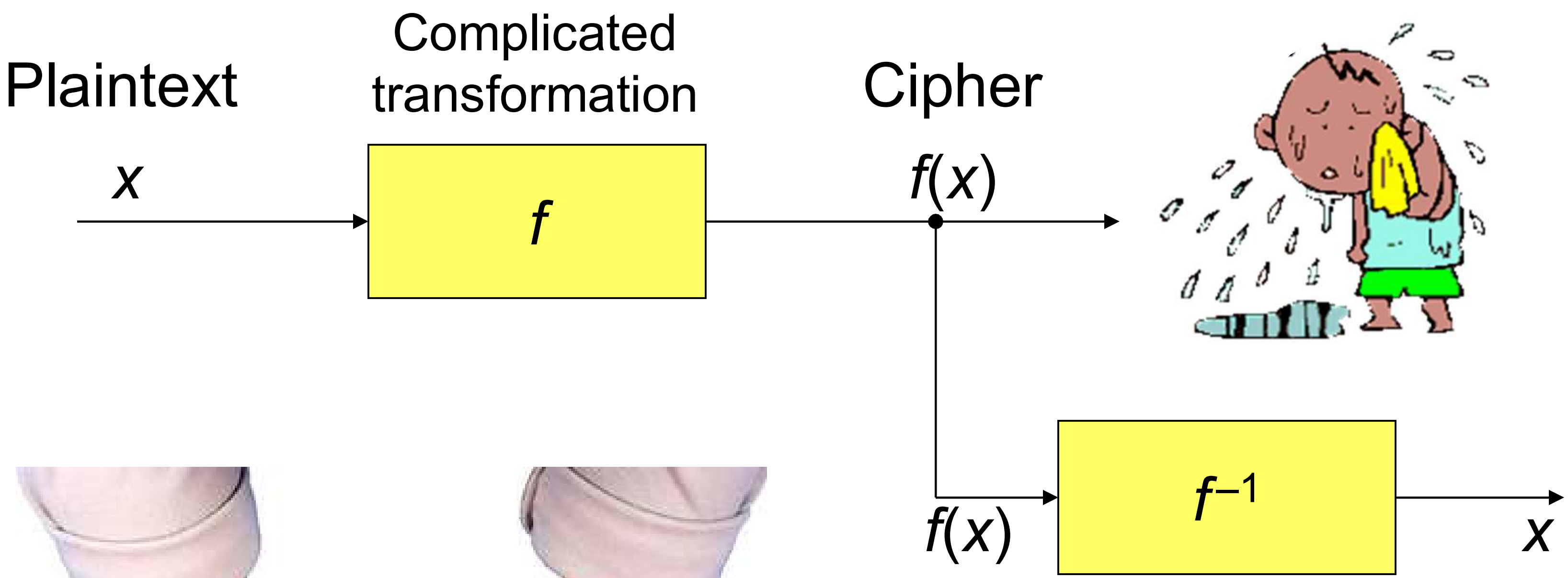




The *f* function is fairly complicated, but it has an efficient hardware realization

Feistel twisted ladder,
Preceded and followed by permutation blocks form DES's encryption, decryption algorithms

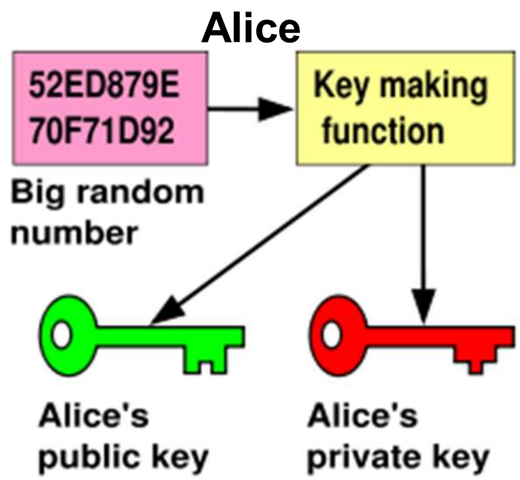
Use of Backdoors in Cryptography



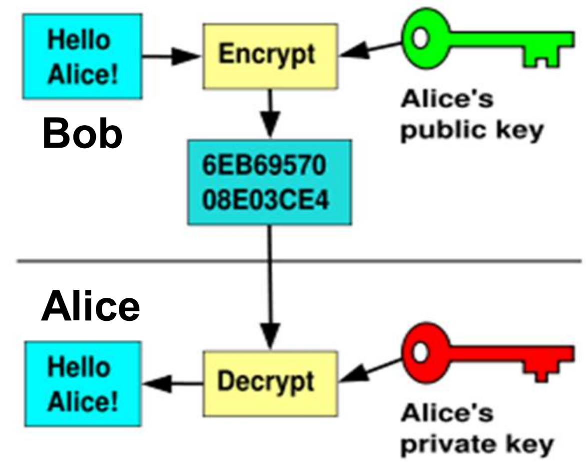
Inverse function is a backdoor . . .

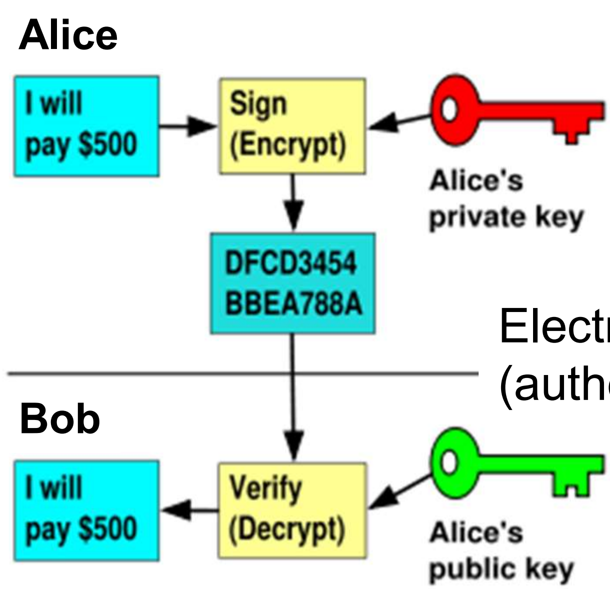
Like a hidden latch that releases a magician's handcuffs

Public-Key Cryptography

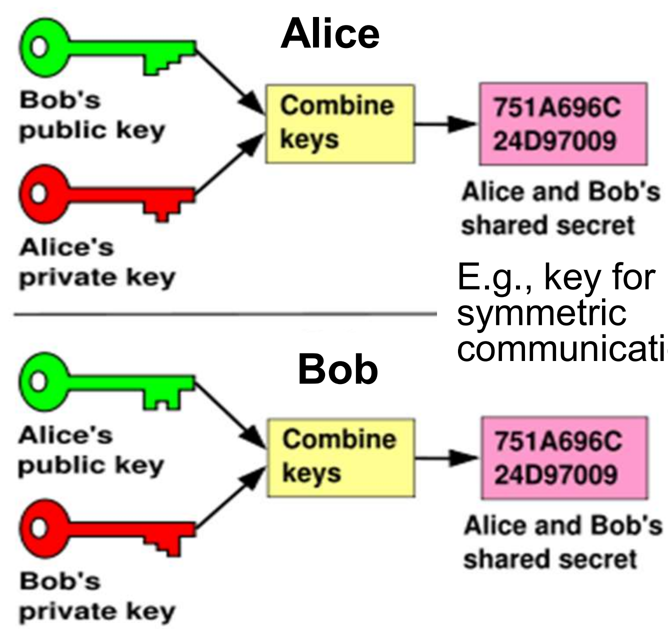


Encryption and decryption are asymmetric. Knowledge of the public key does not allow one to decrypt a message.





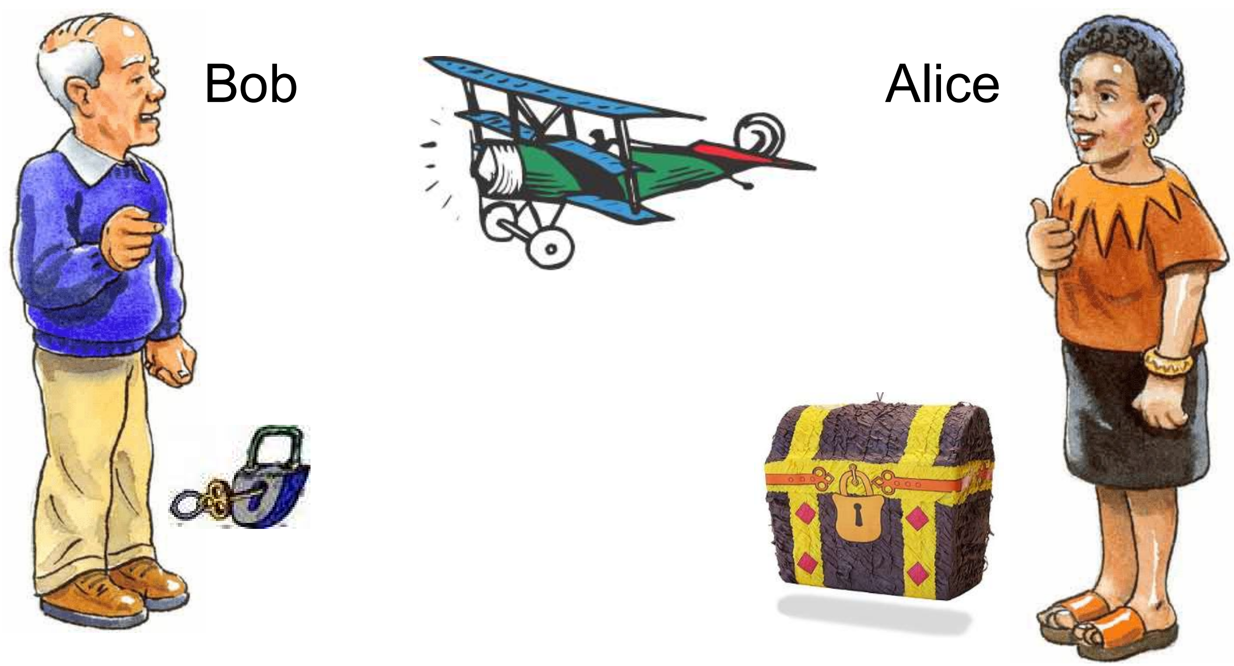
Electronic signature (authentication)



E.g., key for symmetric communication

Source: Wikipedia

Analogy for Public-Key Cryptography



Alice sends a secret message to bob by putting the message in a box and using one of Bob's padlocks to secure it.
Only Bob, who has a key to his padlocks, can open the box to read the message.

RSA Public Key Algorithm

Choose large primes p and q	$p = 7$, $q = 19$
Compute $n = pq$	$n = 7 \times 19 = 133$
Compute $m = (p - 1)(q - 1)$	$m = 6 \times 18 = 108$
Choose small e coprime to m	$e = 5$
Find d such that $de = 1 \bmod m$	$d = 65$
Publish n and e as public key	Public key: 133, 5
Keep n and d as private key	Private key: 133, 65

Security of RSA is due to the difficulty of factoring large numbers
Therefore, p and q must be very large: 100s of bits

Encryption example:

$$y = x^e \bmod n$$
$$= 6^5 \bmod 133$$
$$= 7776 \bmod 133$$
$$= 62$$

Decryption example:

$$x = y^d \bmod n$$
$$= 62^{65} \bmod 133$$
$$= 62(3844)^{32} \bmod 133$$
$$= 62(120)^{32} \bmod 133 = \ldots = 6$$