Cryptography for Dummies
From Classical to Modern

Laszlo Csirmaz

Central European University

March 26–30, 2012

Classic Definition of Cryptography

Cryptography, or the art of "hidden writing," comes from Greek hiding the contents or existence of messages from and adversary

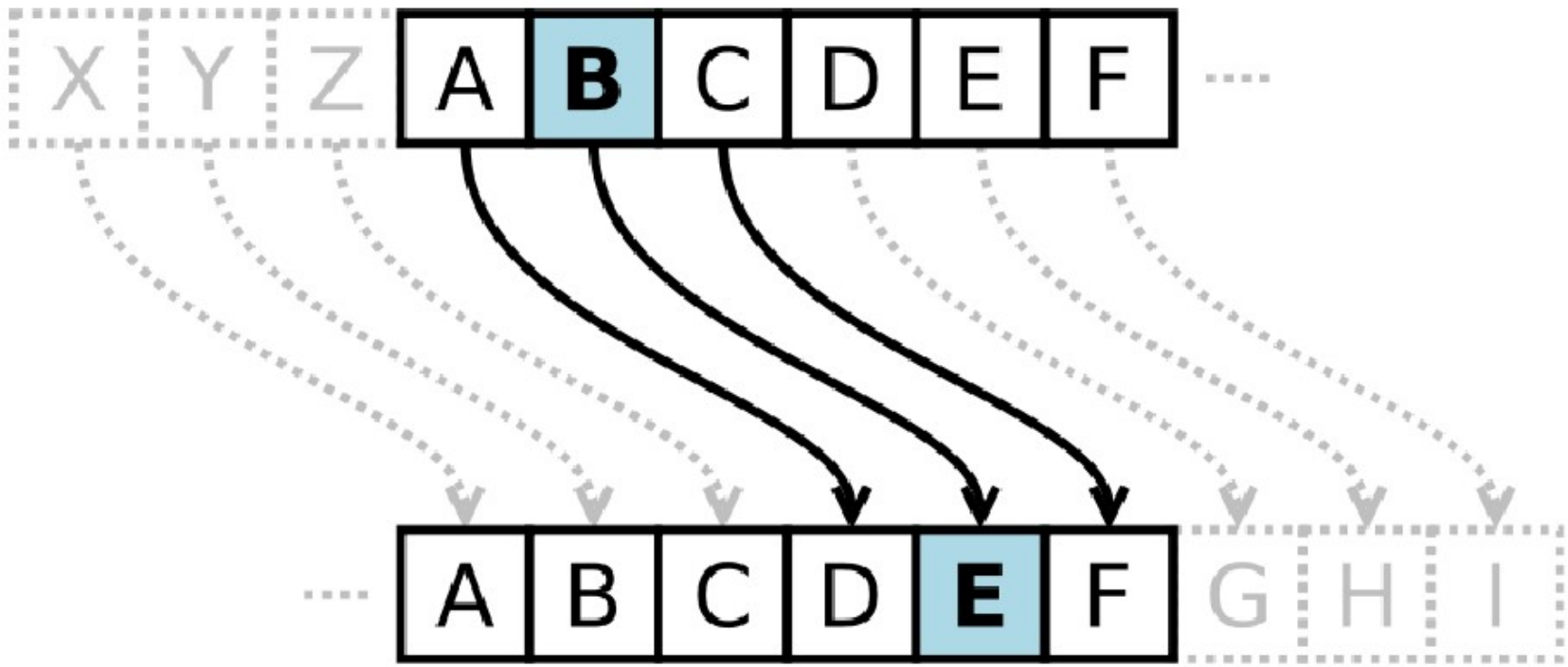
Encryption makes a message unintelligible to anyone not possessing some secret information

Decryption undoes the scrambling

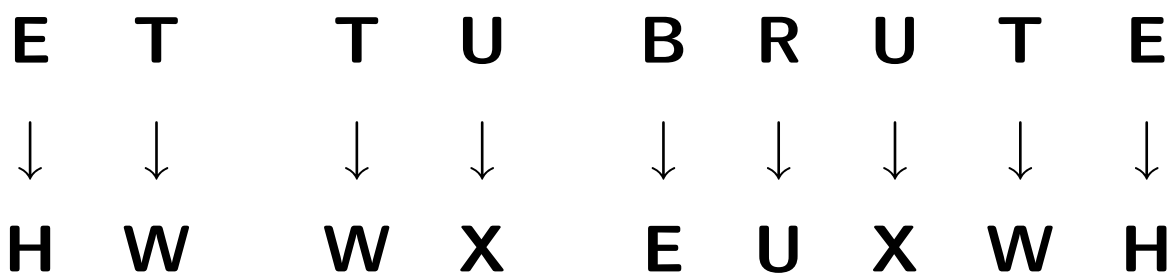
Steganography, or "covered writing," is concerned with hiding the existence of a message – often in plain sight.

Scytale transposition cypher

Caesar Substitution Cipher



Caesar Substitution Cipher

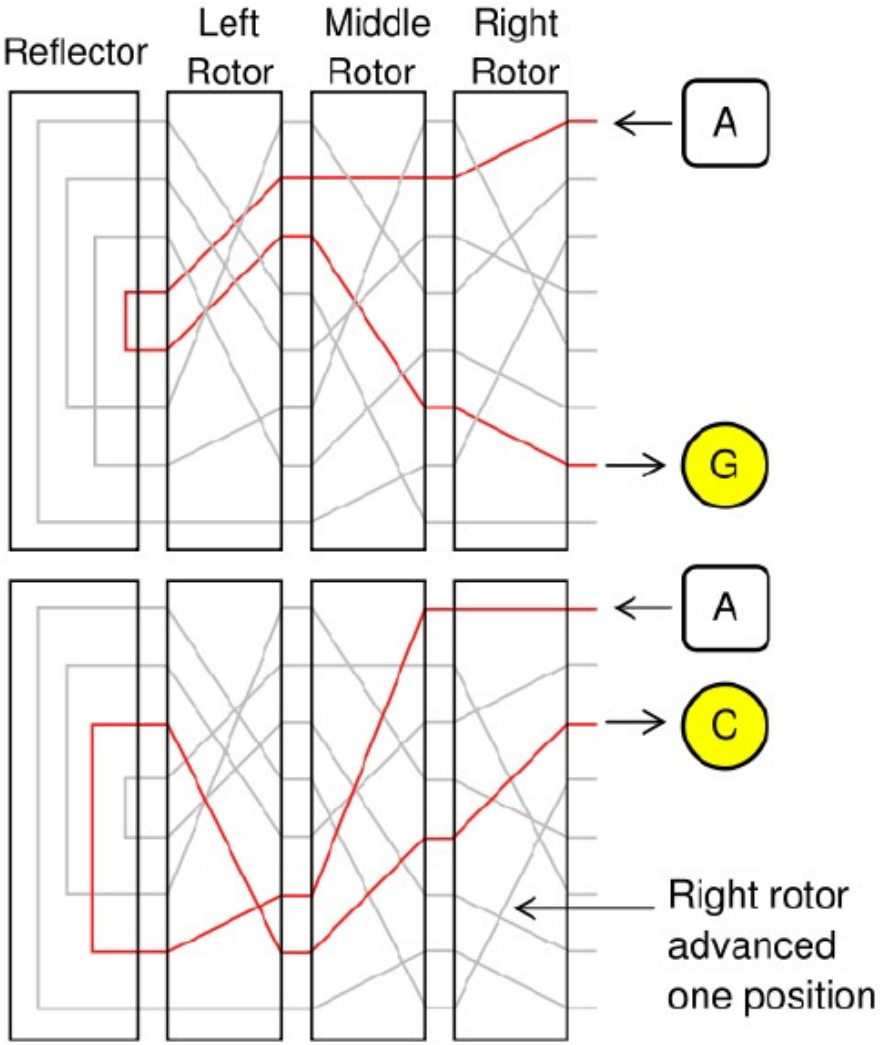


Vigenère Polyalphabetic Substitution

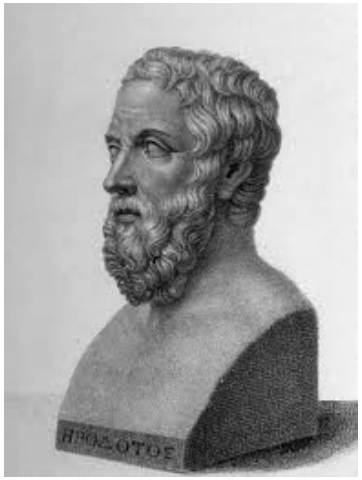
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Key:
SECRET
Plaintext:
PARTY TODAY
Ciphertext:
HETKC MGHAP

Enigma machine



Steganography



- Herodotus tattoo and wax tablets
- invisible ink
- microdots
- “The Finger”
- Low order bits

Code book

Codes replace a specific piece of plaintext with a certain code word. They can also replace several letters at once.

- “Yes” if by land, “no” if by sea
- Beale code
- number stations
- electronic code book (ECB) mode

Kerckhoff's Principle

A cryptosystem should be secure even if everything about it is public knowledge except the secret key.

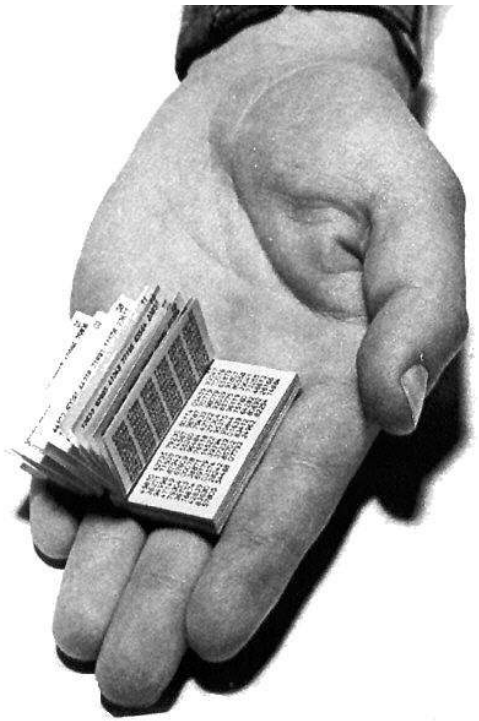
It contrasts to "security through obscurity."

KeeLoq® used by: Chrysler, Daewoo, Fiat, GM, Honda, Jaguar, Toyota, Volvo, WV

Attack: Listen in a parking lot for about 60 minutes, then use your computer for two days. Scary, isn't is?

One-time pads

- Invented several times before and after the II Word War
- used even through the cold war
- *one time* means *one time*
- needs separate keys for each message, and for each recipient
- keys are as big as messages (disposable keypads)



Problems with Classical Crypto

- **weak**: pen-and-paper, and mechanical systems became weak in face of modern computers.

Problems with Classical Crypto

- **weak**: pen-and-paper, and mechanical systems became weak in face of modern computers.
- **informal**: construction was ad hoc. They were not publicly available, there were no "proof" for fit, no definition for what they were good.

Problems with Classical Crypto

- **weak**: pen-and-paper, and mechanical systems became weak in face of modern computers.
- **informal**: construction was ad hoc. They were not publicly available, there were no "proof" for fit, no definition for what they were good.
- **closed**: knowledge and technology available to military and intelligence agencies.

Problems with Classical Crypto

- **weak**: pen-and-paper, and mechanical systems became weak in face of modern computers.
- **informal**: construction was ad hoc. They were not publicly available, there were no "proof" for fit, no definition for what they were good.
- **closed**: knowledge and technology available to military and intelligence agencies.
- **key distribution**: the number of keys grow enormously with the number of participants.

Modern Cryptographic Era

- cryptography now is an everyday commodity
- new cryptographic primitives
- asymmetric and public cryptosystem
- standardization, formalization
- internet and wireless communication
- liberalization of cryptographic restrictions

Cryptography Topics

- Key Distribution Problem
  How Alice and Bob first agree on a shared key?

Cryptography Topics

- Key Distribution Problem
  How Alice and Bob first agree on a shared key?
- **MIM** attack (man in the middle)

Cryptography Topics

- Key Distribution Problem
  How Alice and Bob first agree on a shared key?
- **MIM** attack (man in the middle)
- Public Key Encryption
  Diffie–Hellman, RSA
  How do you get the public keys?
  Why should you trust the encrypted message?
  How will you know that is was *not* modified?

Cryptography Topics

- Key Distribution Problem
  How Alice and Bob first agree on a shared key?
- **MIM** attack (man in the middle)
- Public Key Encryption
  Diffie–Hellman, RSA
  How do you get the public keys?
  Why should you trust the encrypted message?
  How will you know that is was *not* modified?
- Authentication
  How do you know that a message was sent by your bank?
  How do you know that it has not been altered?