FYSE 1280
BREAKING THE CODE:
THE ENGIMA OF ALAN TURING

Introduction to Cryptology I

Cryptology and Computer Security

Why Should You Be Interested in Cryptology?

Historical Importance

Military

Diplomatic

Contemporary Importance

Data Protection

Secure Communications

Governments

The Hotline

Banking and Funds Transfers

Email Privacy

Payments via Browsers

Cable TV and Scrambled Signals

Passwords and "Logging On"

Digital Cash and Smart Cards

Cellular Phones

The McVeigh Execution

Vehicle to Study Mathematical Topics

Number Theory	Linear Algebra
Discrete Mathematics	Computers
Probability and Statistics	Logic

Intellectual Stimulation

Many Open Research Questions

Links to Other Disciplines

Engineering and Linguistics

References

Simon Singh, *The Code Book*, Doubleday 1999.

David Kahn, T*he Codebreakers*, Macmillan 1967; second edition, 1992.

David Kahn, *Seizing the Enigma*, Houghton-Mifflin, 1991.

Steven Budiansky, *Battle of Wits: The Complete Story of Code Breaking in WWII*, The Free Press, 2000.

Our Goal

Review some of the classic methods inclduing ENIGMA and learn enough about their underlying mathematics so we can appreciate the most important current public-key system: The RSA Algorithm.

CRYPTOLOGY

CRYPTOGRAPHY

Hiding the meaning

of messages

CRYPTANALYSIS

Discovering the meaning

of intercepted messages

CRYPTOGRAPHY

A) HIDING THE EXISTENCE OF A MESSAGE

Steganography

Invisible Ink

Microdots

Pinholes

Examples of Steganography

B) HIDING THE MEANING OF A MESSAGE

Transpositions

Substitutions

SUBSTITUTIONS

CODES

CIPHERS

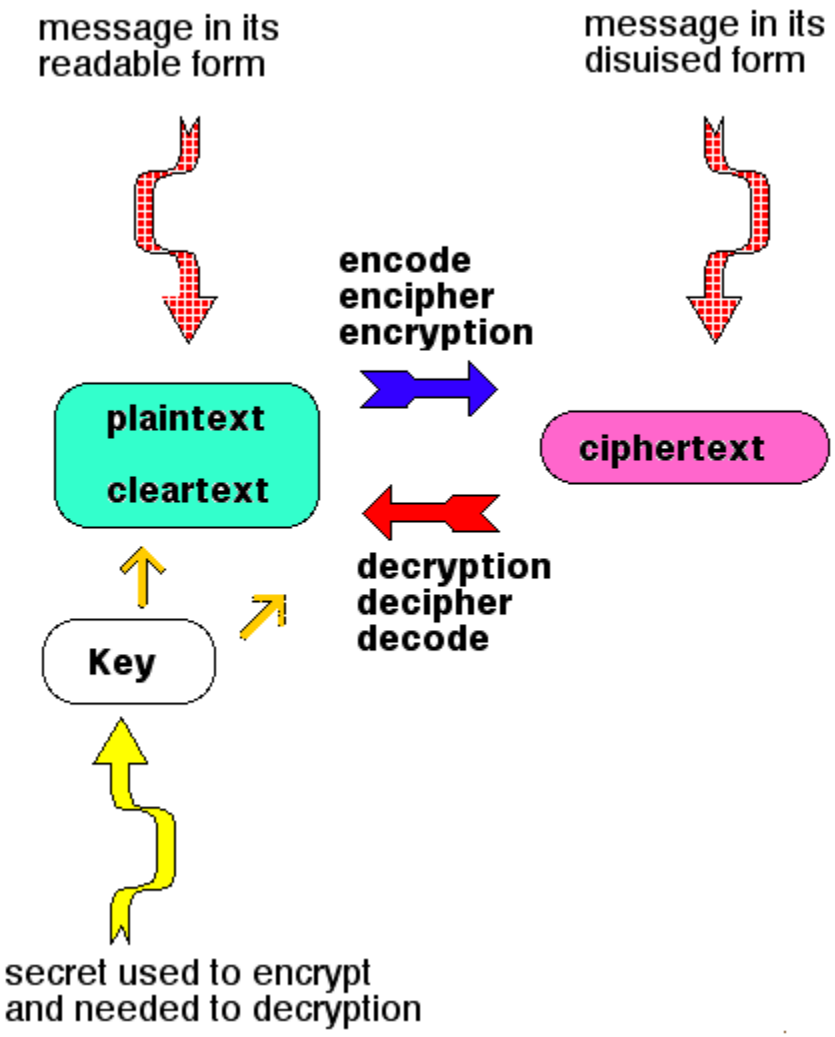
CODES

plaintext	**ATTACK AT DAWN**
coded text	**15921 24586 49198**

CIPHERS

Example: Replace each letter by the next one in the alphabet

plaintext	**ATTACK AT DAWN**
ciphertext	**BUUBDL BU EBXO**



CIPHERS

MONALPHABETIC SUBSTITUTION

POLYALPHABETIC SUBSTITUTION

POLYGRAPHIC SYSTEMS

MONALPHABETIC SUBSTITUTION

Caesar Cipher: Replace each letter of the message by the letter **3** places beyond it in the normal alphabet.

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

AT T ACK AT DAWN

DWWDFN DW GD ZQ

Method: Shift by *x* characters

Key: value of *x*

Numerical Implementation of Classic Caesar Cipher

1) Replace each letter by its position in the alphabet

2) Add *3* modulo 26 to the position

3) Replace resulting number by its letter equivalent

M --> 13 --> 16 --> **P**

Caesar.html

Cracking a Caesar Cipher by "Brute Force"
Find the Key by Trying All Possibilities

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

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

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

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

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

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