CODING/DECODING

first use of the term `cryptograph': The Gold Bug, a novel by E. Poe

ENCRYPTION

plaintext

ordinary information

algorithm

ciphertext

unintelligible form

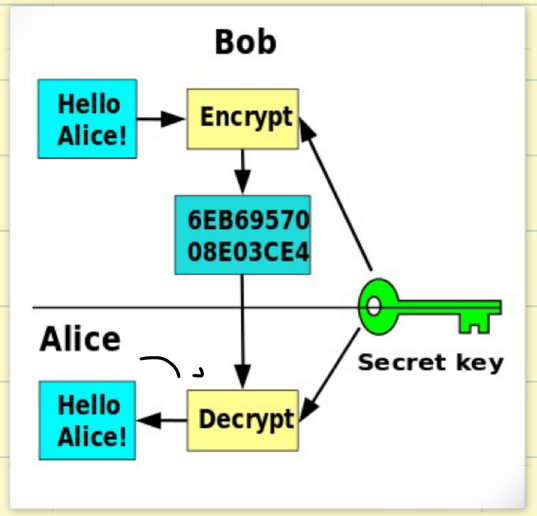
cipher (or cypher)

decryption goes the other way

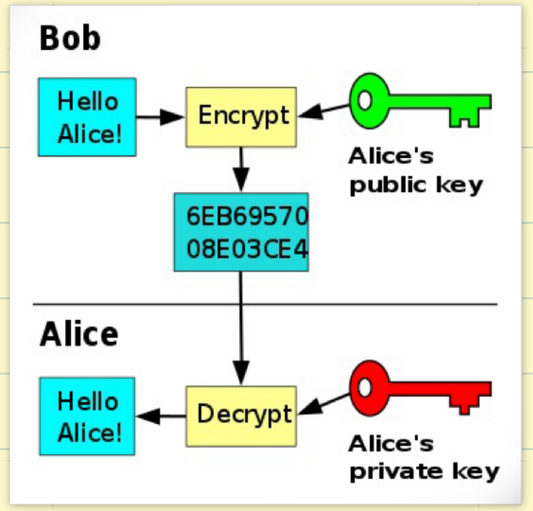
(70s)

Hybrid systems prefered

Symmetric cipher



Asymmetric cipher



message: symmetric

secret key: assymetric

Algorithm: RSA, AESAESAES

Same key for encryption and decryption

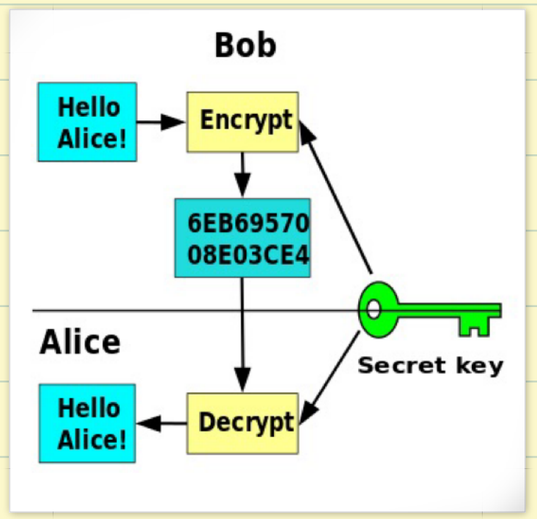
Drawback: easier to break

Different keys used for encryption and decryption

Drawback: computationally more expensive

Symmetric vs asymmetric

Symmetric cipher



Same key for encryption and decryption

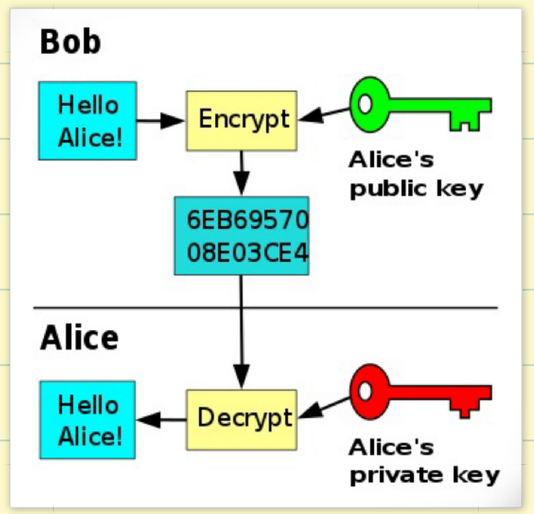
Examples

Caesar cipher

Vinegere cipher

this lecture

Asymmetric cipher (70s onwards)



Different keys used for encryption and decryption

Algorithm: RSA, AESAESAES

Hybrid systems prefered

message: symmetric
key: asymmetric

Drawback: computationally more expensive

Caesar cipher

Named after J. Caesar who invented it

Each letter of the alphabet is shifted along some number of places

ENCRYPTION formula

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

- cipher character
- shift (key)
- plain text
- if a letter is shifted past the alphabet it wraps around the beginning

Example

p: Hello world

k: 3

c : Khoor zruog

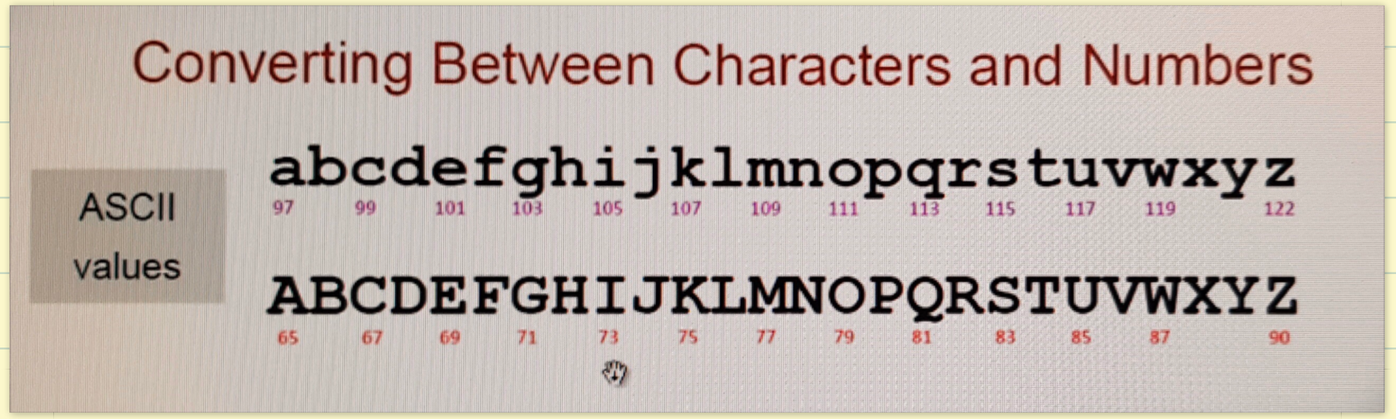
sample calculation. H is 7. (7+3) mod 26 = 10. This is K

A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7
I 8	J 9	K 10	L 11	M 12	N 13	O 14	P 15
Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23
Y 24	Z 25						

DECRYPTION formula $p = (c-k) \bmod 26$

sample decryption. K is 10. (10-3) mod 26 = 7 mod 26 = 7. This H.

Caesar cipher in python



ord(): returns the ascii value of a given character

chr(): returns the character corresponding to a value

SEE FILE CAESAR.PY

Brute force attack

VIGENERE CIPHER

- Improves Caesar cipher
- Used during American civil war
- 3 centuries to break it
- Polyalphabetic substitutions
  series of interwoven Caesar ciphers

plain text → ATTACKATDAWN

Key → LEMONLEMONLE (same lenght as plain text)

cipher text → LXFOPVEFRNHR

plain text →

key ↓	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	T	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

TABULA RECTA

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

$(0 + 11) \bmod 2$

$= 11 \bmod 26$

$= 11$

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

$(11 - 11) \bmod 26$

$= 0 \bmod 26$

$= 0$

A_0 B_1 C_2 D_3 E_4 F_5 G_6 H_7

I_8 J_9 K_{10} L_{11} M_{12} N_{13} O_{14} P_{15}

Q_{16} R_{17} S_{18} T_{19} U_{20} V_{21} W_{22} X_2

Y_{24} Z_{25}