UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

HUMAN INSPIRED TECHNOLOGY Research Centre

DIPARTIMENTO MATEMATICA

Cryptographic Properties of XOR

What we already know...

XOR

$0\ 0 \rightarrow 0$

$0\ 1 \rightarrow 1$

$1\ 0 \rightarrow 1$

$1\ 1 \rightarrow 0$

Repeating XOR cipher

enc_message = clear_message ^ key

Repeating XOR cipher

enc_message = clear_message ^ key

clear_message = “THIS IS A MESSAGE”
key = “YOU”

T	H	I	S		I	S		A		M	E	S	S	A	G	E
Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O

Repeating XOR cipher

enc_message = clear_message ^ key

clear_message = “THIS IS A MESSAGE”
key = “YOU”

T	H	I	S		I	S		A		M	E	S	S	A	G	E
84	72	73	83	32	73	83	32	65	32	77	69	83	83	65	71	69

Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O
89	79	85	89	79	85	89	79	85	89	79	85	89	79	85	89	79

Repeating XOR cipher

enc_message = clear_message ^ key

clear_message = “THIS IS A MESSAGE”
key = “YOU”

clear_message	84	72	73	83	32	73	83	32	65	32	77	69	83	83	65	71	69
key	89	79	85	89	79	85	89	79	85	89	79	85	89	79	85	89	79
enc_message	13	7	28	10	111	28	10	111	20	121	2	16	10	28	20	30	10

84 = 1010100
89 = 1011001
13 = 0001101

Properties of the XOR cipher

- XOR is commutative
  a ^ b = b ^ a

- XOR is associative
  a ^ (b ^ c) = (a ^ b) ^ c

- Anything XORed with itself is zero
  a ^ a = 0

- Anything XORed with zero is anything
  a ^ 0 = a

Properties of the XOR cipher

enc_message = clear_message ^ key

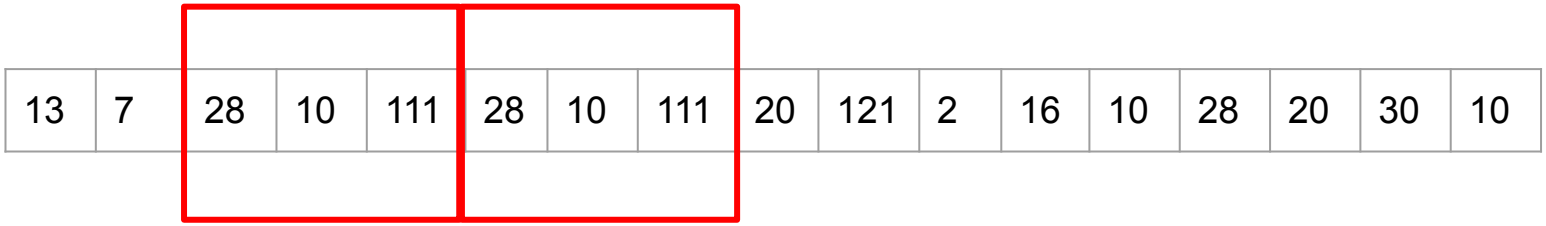
clear_message = enc_message ^ key

key = clear_message ^ enc_message

Kasiski elimination

13	7	28	10	111	28	10	111	20	121	2	16	10	28	20	30	10

Kasiski elimination



Kasiski elimination

13	7	28	10	111	28	10	111	20	121	2	16	10	28	20	30	10

T	H	I	S		I	S		A		M	E	S	S	A	G	E
Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O

ord('I') ^ ord('U') = 28
ord('S') ^ ord('Y') = 10
ord(' ') ^ ord('O') = 111

Kasiski elimination

Kasiski elimination

13	7	28	10	111	28	10	111	20	121	2	16	10	28	20	30	10

T	H	I	S		I	S		A		M	E	S	S	A	G	E
Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O

clear_message(i) ^ key(i) = 28
clear_message(i + 1) ^ key(i + 1) = 10
clear_message(i +2) ^ key(i +2) = 111

XOR in Python

Standard instruction to compute a XOR in Python. The result is a vector of numbers.

enc_message = [i ^ j for i, j in zip(clear_message, key)]

i and j should be integers

If you want the output as a string

enc_message = ''.join([chr(i ^ j) for i, j in zip(clear_message, key)])