Grand Theft Crypto

Florida Tech IoT S&P Lab

Alan Turing: Crypto Hero

Alan Turing was a computer scientists and mathematician who worked at Bletchley Park (Great Britain's Code Breaking Center.)

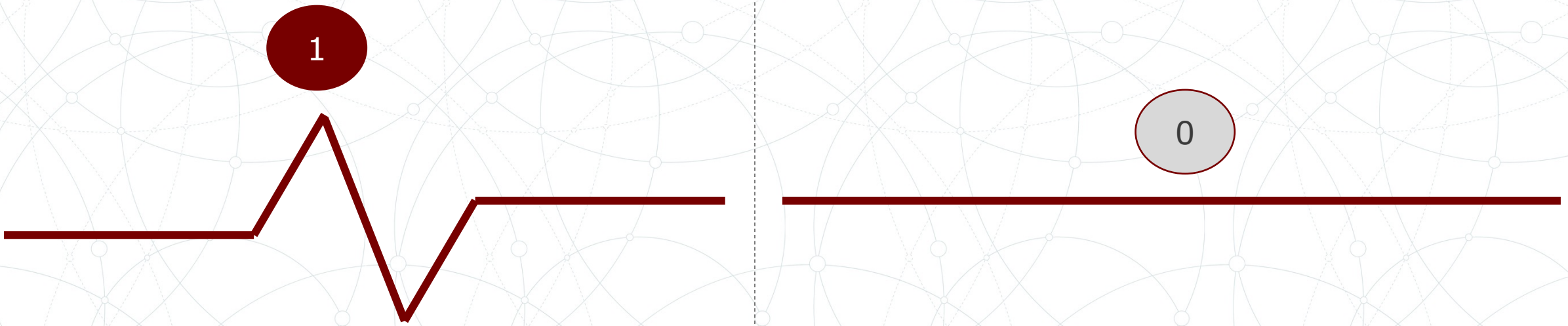
He attacked the German Cryptographic Systems.

By all accounts, he saved millions of lives and four years of war by defeating the German U-bots cryptographic system.

Today we will learn to hack like Alan and attack crypto systems. First, some small background.

FLORIDA TECH

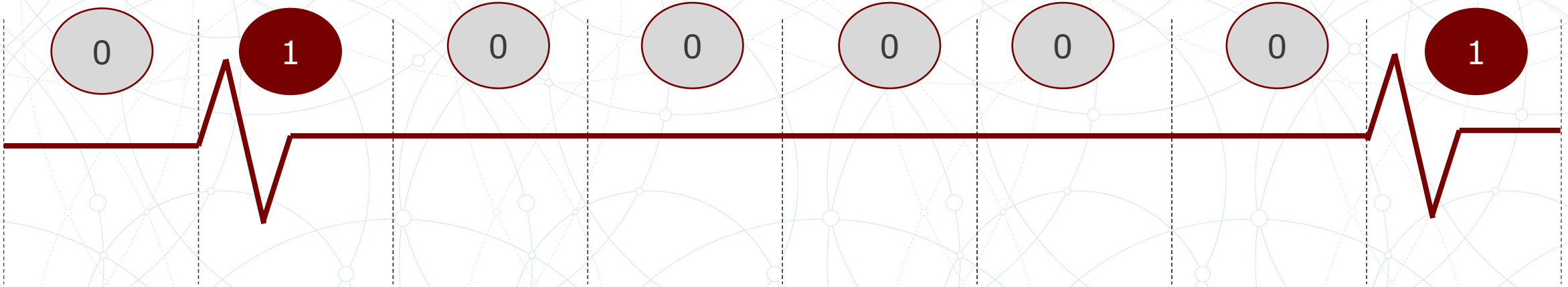
Binary Data



Binary refers to a number system where there are only two possible outcomes (1 or 0). Computers use transistors and capacitors to store electrical charges. These charges represent either a 1 or a 0. A bit represents a single outcome.

FLORIDA TECH

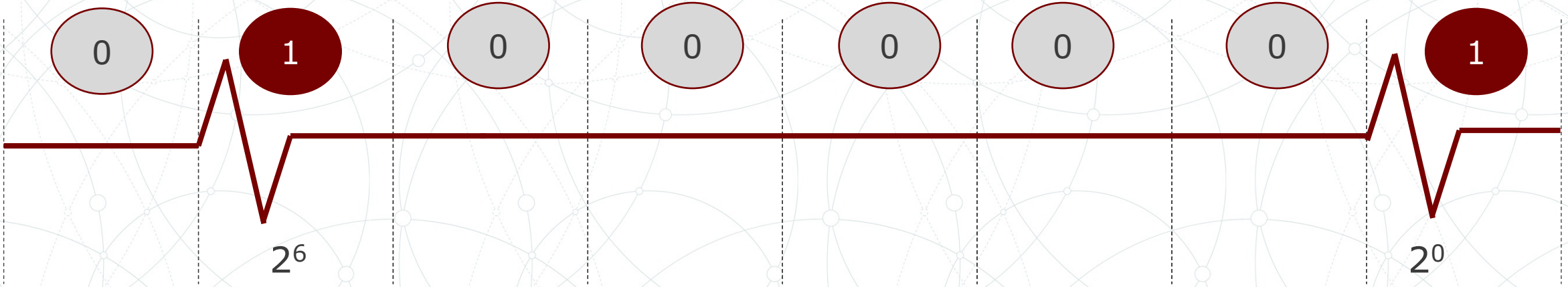
Bits to Bytes



We called groupings of 8 bits a byte. Since each bit can have two possible outcomes, a byte can store $2^8 = 256$ possible values.

FLORIDA TECH

Bytes to Decimal



To convert bytes to decimal (base 10 numbering), we sum each enabled bit raised to the power of its position. So, 01000001 = 2^6+2^0 = 64 + 1 = 65

FLORIDA TECH

Decimal to ASCII

```
>>> import string

>>> print(string.printable)
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

>>> print(len(string.printable))
100

>>> chr(65)
'A'
```

Since computers can't store letters, they just create tables to represent letters, where each letter has a specific decimal value. For example, the number 65 represents the letter A and the number 66 represents B.

A	B	C	…	a
65	66	67	…	97

FLORIDA TECH

Encryption: Plaintext

When we transmit data over communication lines (radio, internet, …), if its in its original form (also known as plaintext), our enemies may be able to intercept and read it.

FLORIDA TECH

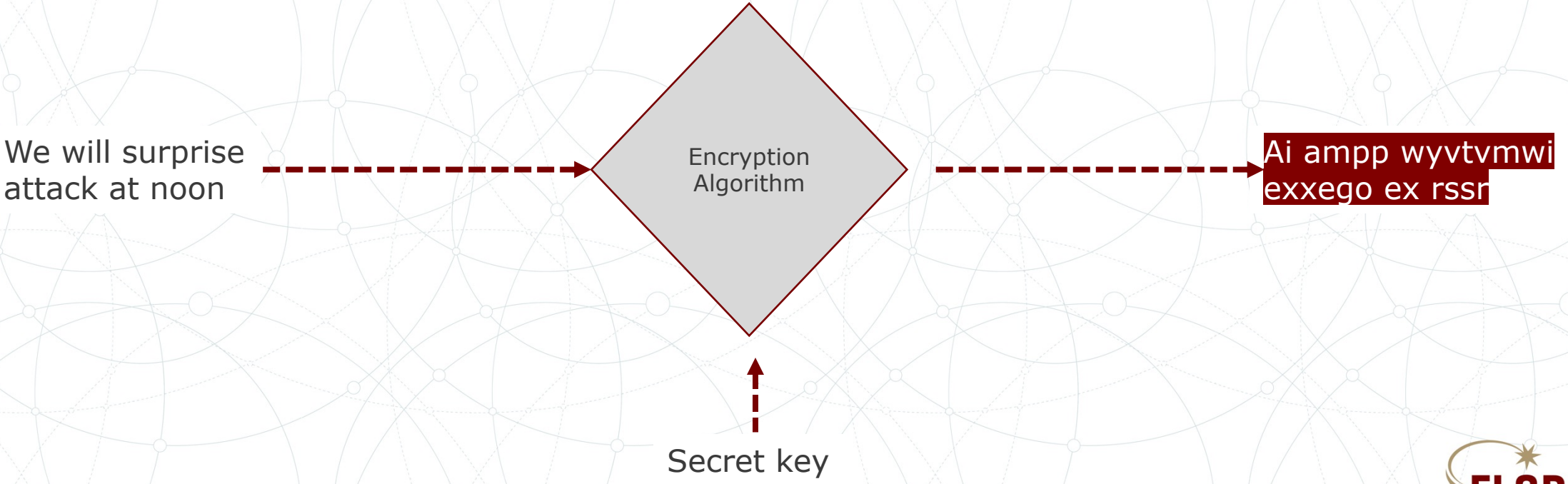
Encryption: Ciphertext

We use encryption to represent the data in a form (ciphertext) that will obscure the original (plaintext) message.

Ai ampp wyvtvmwi exxego ex rssr

Encryption: Algorithms

Encryption algorithms take plaintext messages and convert them to ciphertext. They can also take ciphertext messages and convert them to platinext using decryption.



FLORIDA TECH

Permutation

Substitution

We will surprise
attack at noon

We w|ill |surp|rise| att|ack |at n|oon |

W ew| lli|prus|esir| tta| kca|n ta| noo|

W ew lliprusesir tta kcan ta noo

ABCDEFGHIJKLMNOPQRSTUVWXTZ
DEFGHIJKLMNOPQRSTUVWXTZABC

We will surprise attack at noon

Zh zloo vxusulvh dwwdfn dw qrrq

We can use permutation or substitution ciphers to encrypt data. Permutation rearranges the order of the letters. Substitution replaces the letters with new letters.

FLORIDA TECH

Symmetric Key

FLORIDA TECH

Symmetric Key

Symmetric key algorithms encrypt data by having the recipients agree on a pre-shared key. The same key is used for encryption and decryption. This uses a little math, so let us learn about it.

Key: s3cr3t*k3y*

Key: s3cr3t*k3y*

FLORIDA TECH

XOR Boolean Operation

A	B	Result
0	0	0
0	1	1
1	0	1
1	1	0

A = B → 0
A != B → 1

XOR is a Boolean logic operation that we use in cryptography. Its pretty simple, we compare two bits, if they are the same the result is a 0. If they are different, the result is a 1.

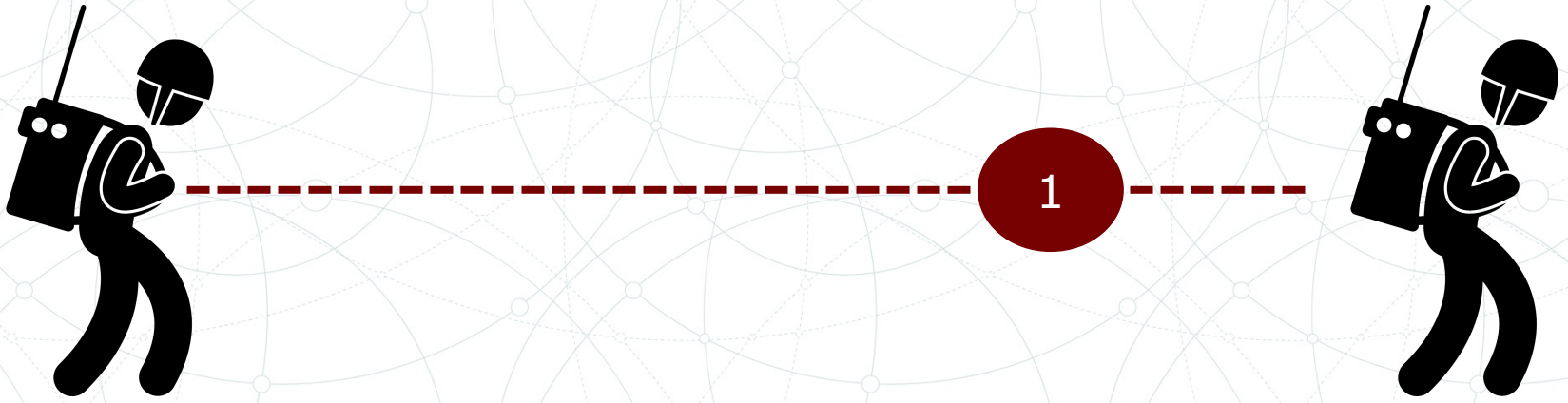
FLORIDA TECH

XOR Symmetric Key

A = B → 0
A != B → 1

Plaintext	Key	Ciphertext
0	0	0
0	1	1
1	0	1
1	1	0

Imagine a soldier transmitted a ciphertext message of ”1” that was XOR encrypted with the key “1”. What was the original plaintext message?



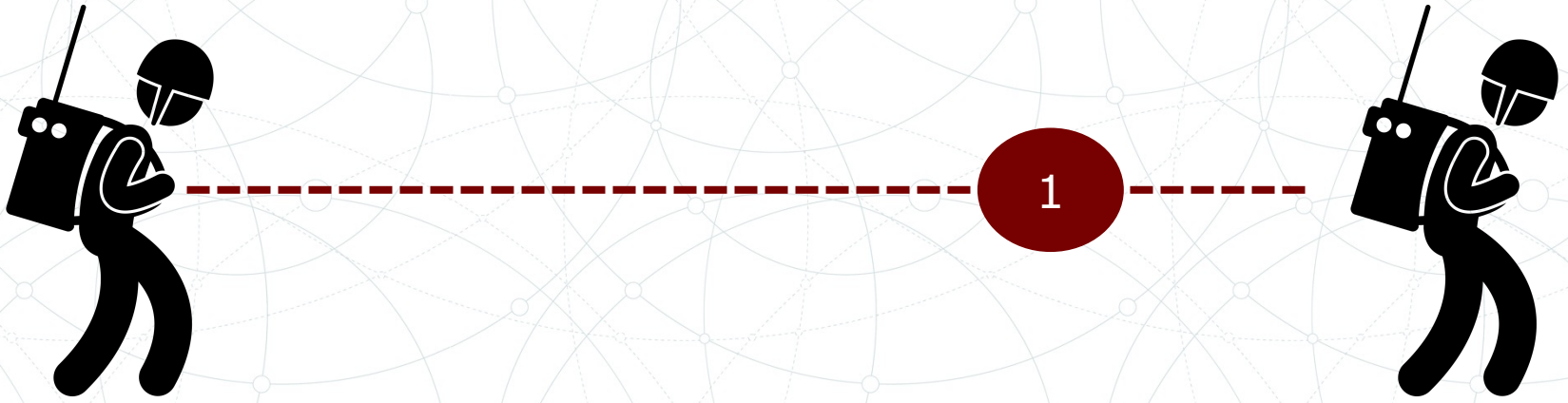
FLORIDA TECH

XOR Symmetric Key

A = B → 0
A != B → 1

Plaintext	Key	Ciphertext
0	0	0
0	1	1
1	0	1
1	1	0

Imagine a soldier transmitted a ciphertext message of ”1” that was XOR encrypted with the key “1”. What was the original plaintext message?



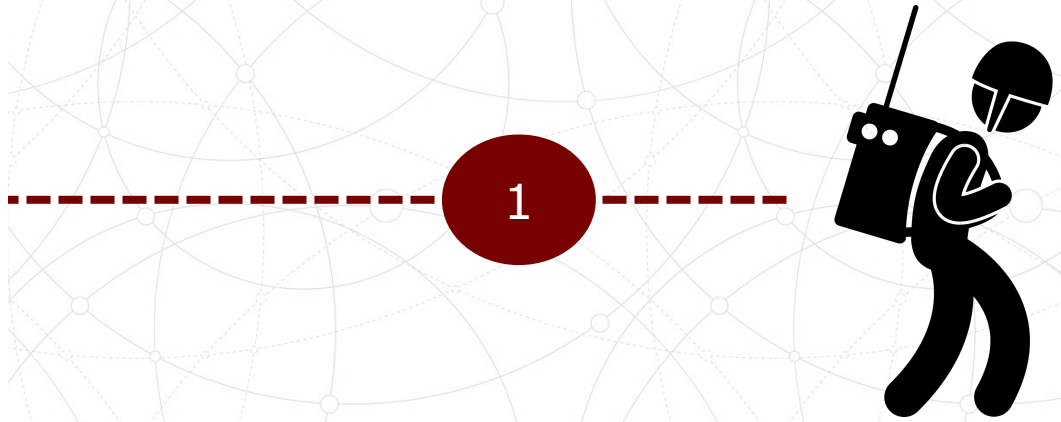
FLORIDA TECH

XOR Symmetric Key

A = B → 0
A != B → 1

Plaintext	Key	Ciphertext
0	0	0
0	1	1
1	0	1
1	1	0

Notice how the soldier CAN ONLY DECRYPT the message if she has the key? Without knowing the key, the plaintext could be a 1 or 0.



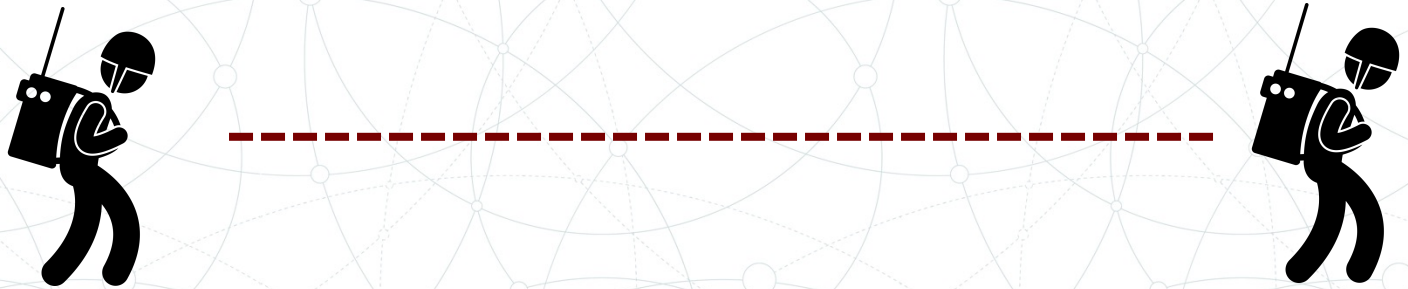
FLORIDA TECH

Known Plaintext Attack

There exists an attack known as a “known plaintext” attack in which the attacker attempts to recover an encryption key because she knows at least one plaintext message and the corresponding ciphertext? Can you guess how it works?

```
>>> xor(b'Good Morning',b'k3y')
b',\\\x16\x0f\x134\x04A\x17\x02]\x1e'
```

```
>>> xor(b',\\\x16\x0f\x134\x04A\x17\x02]\x1e',b'k3y')
b'Good Morning'
```



FLORIDA TECH

Known Plaintext Attack

That's right! XOR (plaintext, ciphertext) = Key
So if we know the plaintext from AT LEAST ONE of the encrypted messages sent by our enemies, we can determine the key at DECRYPT ALL OF THE MESSAGES.

```
>>> xor(b'Good Morning',b'k3y')
b',\\\x16\x0f\x134\x04A\x17\x02]\x1e'
```

```
>>> xor(b',\\\x16\x0f\x134\x04A\x17\x02]\x1e',b'k3y')
b'Good Morning''
```

```
>>> xor(b',\\\x16\x0f\x134\x04A\x17\x02]\x1e', b'Good Morning')
b'k3yk3yk3yk3y''
```

FLORIDA TECH

Alan Turing: Crypto Hero

Alan Turing used known plaintext attacks too. He called the known plaintext messages cribs since they had predictable content. He used the following crib to help the allied forces intercept the U-boat traffic on D-Day.

WETTERVORHERSAGEBISKAYA
(Weather Forecast Biscay)

FLORIDA TECH

Can You Become A Crypto Hero Too?

FLORIDA TECH

Crypto Hero Exercise Details

Connect to the wireless car via RCCTF-<car id>
Go to http://10.3.141.1 and follow the prompts to attack the car.

Helpful hint #1: a byte is 8 bits; so there are 2^8 possible values for a byte.
Helpful hint #2: xor(encrypted_message,plaintext_message) = key

FLORIDA TECH

FLORIDA TECH

Thank you.