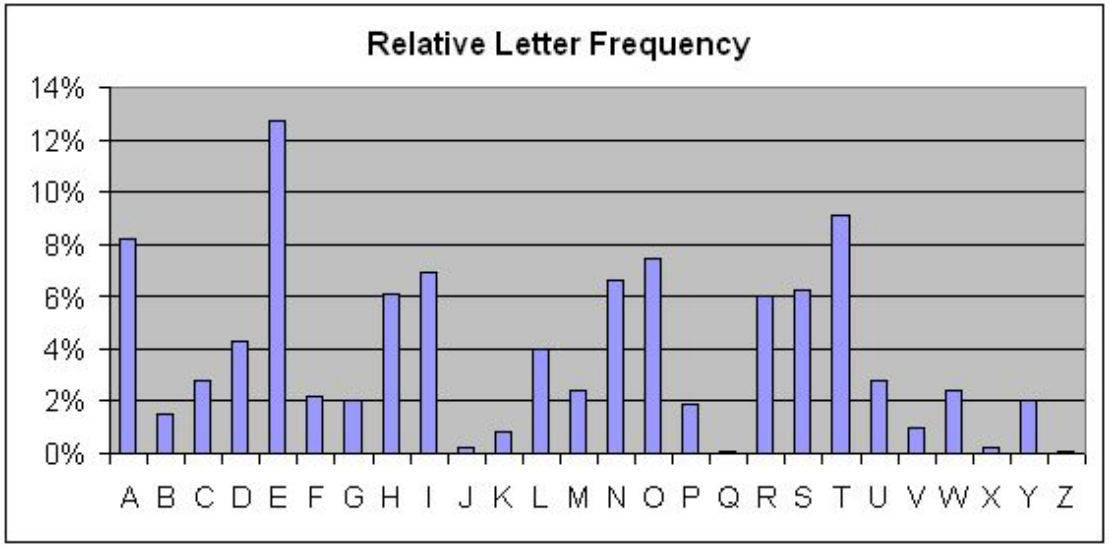
More Encryption

Try to decrypt this using your code!

' GTGVVRKGJGEQKKVYZNKJUIZUXGCGE '

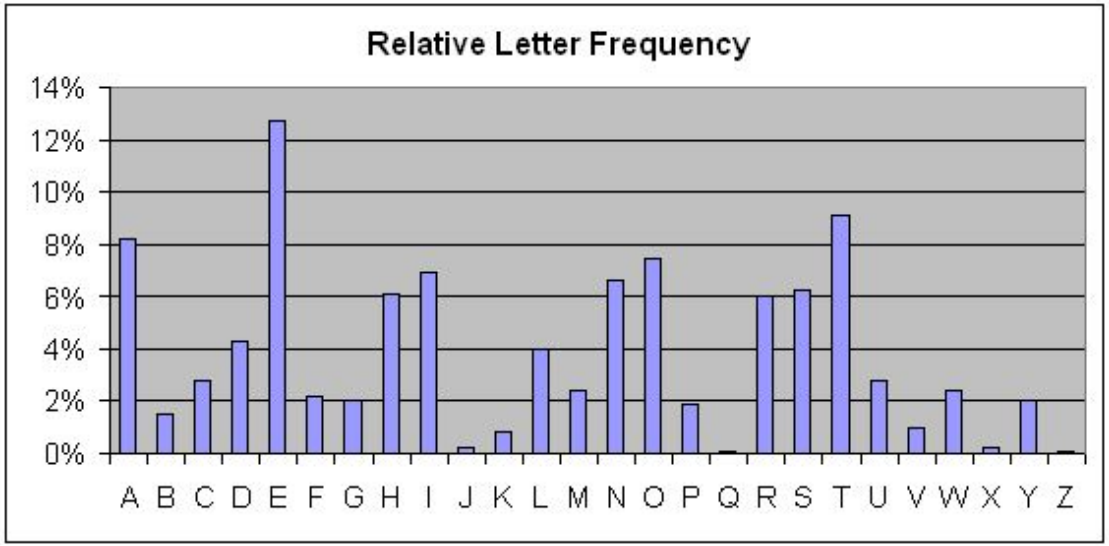
Breaking Caesar Cipher (CryptAnalysis)

' GTGVVRKGJGEQKKVYZNKJUIZUXGCGE '



Breaking Caesar Cipher (CryptAnalysis)

' GTGVVRKGJGEQKKVYZNKJUIZUXGCGE '

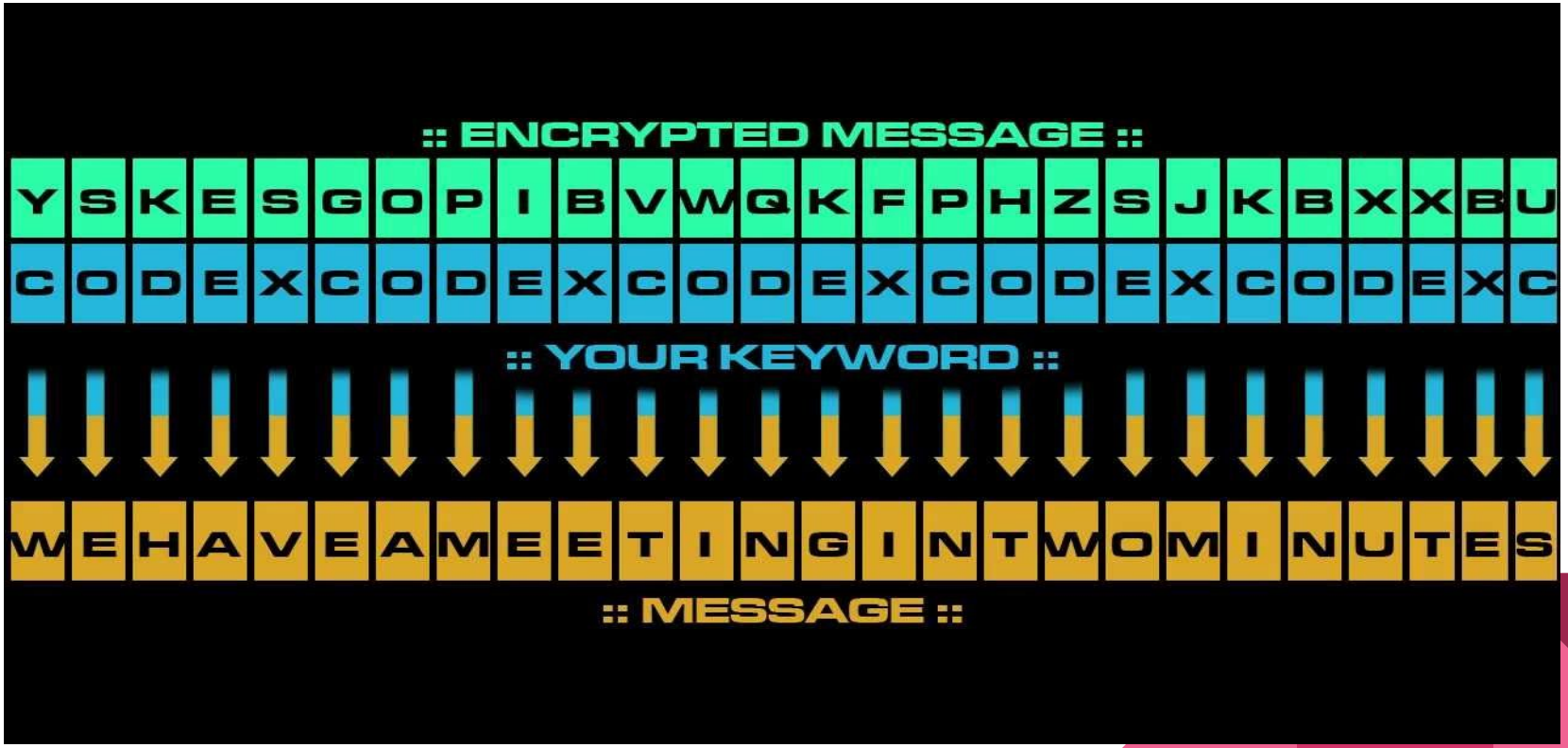


Or just try all 26 option…...

Ciphertext-only attack

- Given a ciphertext, try to figure out the key and the plaintext.

Vigenere Cipher

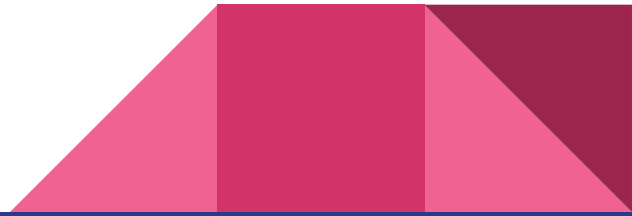


Vigenere Cipher

- You can think Vigenere Cipher as an extended version of Caesar Cipher.
- Instead of using just one letter, you use a phrase.
- For the first letter of the message, shift by the first letter of the key. Second letter of the message by the second letter in the key, etc. If the key ran out of letters, go back to the first letter of the key and keep going.

Vigenere Cipher

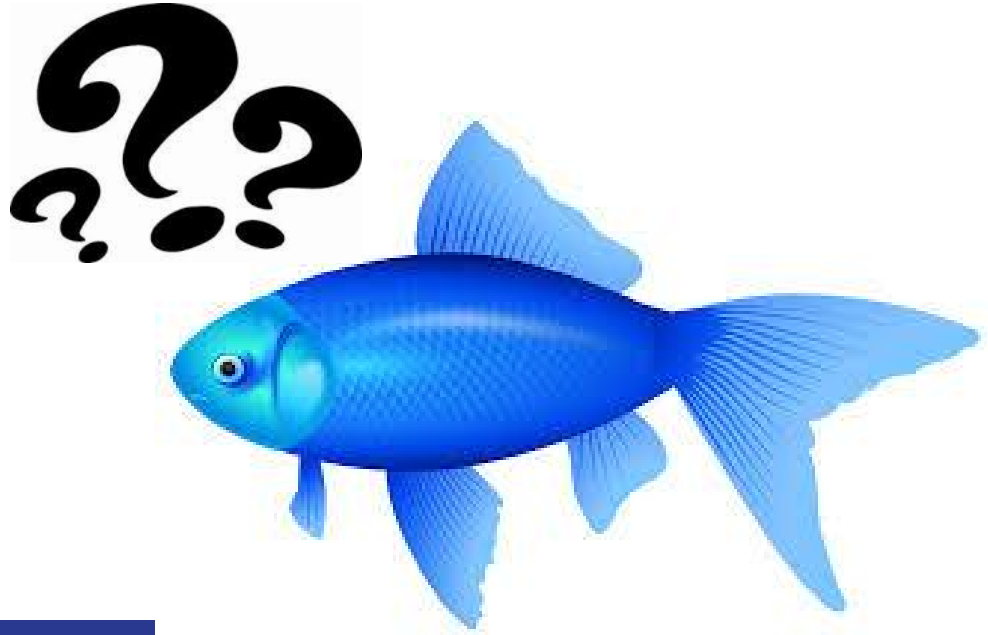
- Was unbreakable for three centuries (not this century)
- Longer keys takes longer time to break.



Try to decrypt this vigenere cipher.

LQNLFUSUFNAZMIFKDWMMJMVONUXVWIVHDBWHHPSTFVLVKQKOFVVFTCXL
JLZPRNGYFTAMJBATJ

I wonder what the key is ?

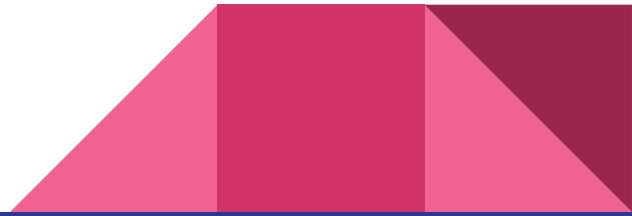


Let’s try another one.

PWWNRHOOLHJCBRLIHHNMNZUCEPYTAHLJOHPXWLUTG
GEFMALTRK

Can we break Vigenere Cipher the same way we break Caesar Cipher?

- Kinda
- First figure out how long the key was
  - Look for repeated phrases (PFV, PDLE, etc.)
- Then run frequency analysis to each of the corresponding letters of the key.
- https://www.youtube.com/watch?v=P4z3jAOzT9I
- MUCH MORE complicated than breaking Caesar Cipher



Vigenere Cipher

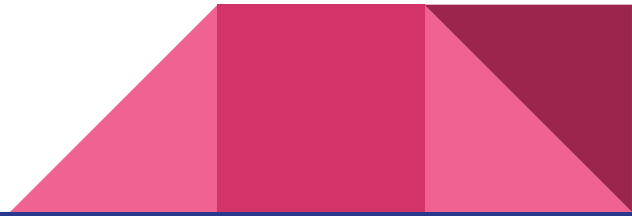
- We are not going to do cryptanalysis of Vigenere Cipher

Vigenere Cipher

- We are not going to do cryptanalysis of Vigenere Cipher
- BUT we are going to implement Encryption and Decryption

Vigenere Cipher

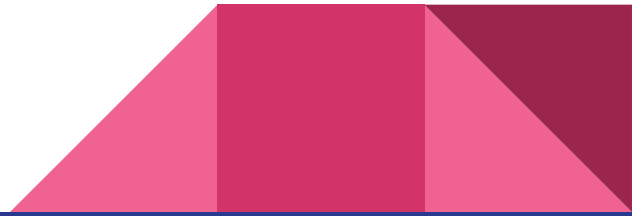
- We are not going to do cryptanalysis of Vigenere Cipher
- BUT we are going to implement Encryption and Decryption
- HINT: You can actually modify your Caesar Cipher Code



Questions for you:

Do you think there is a cipher can achieve perfect secrecy?

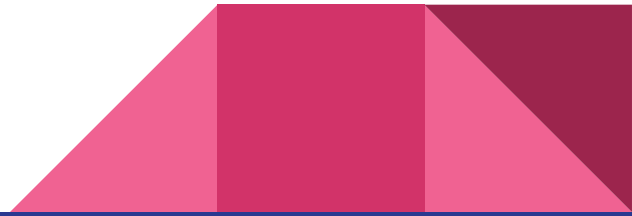
Why or Why not?



One Time Pad

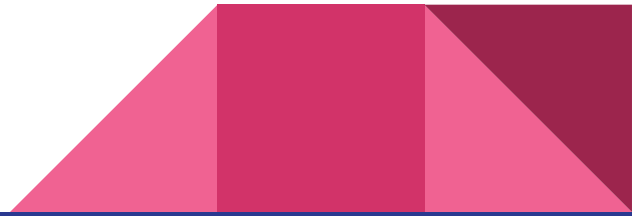
One Time Pad

- If you modify the Vigenere Cipher above a little bit, you can actually get this unbreakable one time pad.



One Time Pad

- **The Key is as long as the message**
- **The Key is random**
- **ONLY use the key once**



One Time Pad

Notice that without the key it is actually **impossible** for the adversary to directly read the message! If you have the ciphertext below, two different keys will get you two different messages:

`EVWSYW OFZ PQWR TP CVIQ`

`attack the hill at dawn`

`EVWSYW OFZ PQWR TP CVIQ`

`attack the barn at noon`

One Time Pad

Notice that without the key it is actually **impossible** for the adversary to directly read the message! If you have the ciphertext below, two different keys will get you two different messages:

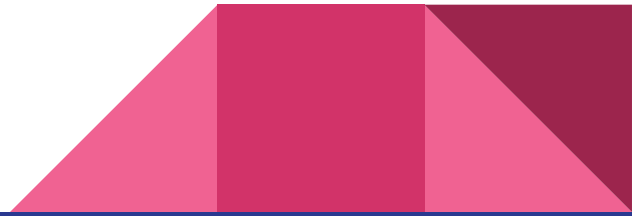
```
EVWSYW OFZ PQWR TP CVIQ          EVWSYW OFZ PQWR TP CVIQ

EOPSAG AGH MWYH CT FVED          EOPSAG HMD QQNE TI PJWD

attack the hill at dawn          attack the barn at noon
```

Shifts never fall into repetitive pattern!

https://www.youtube.com/watch?v=FlIG3TvQCBQ

Your turn

- Implement one time pad (using alphabets)
- You should modify your Vigenere Cipher
- **Key should be as long as the message**
- **Key must be random**



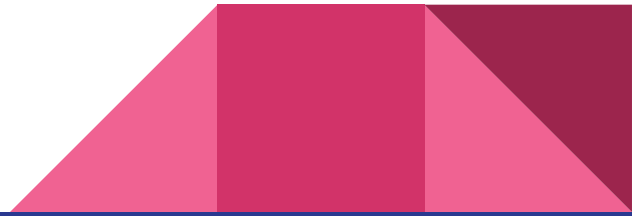
Binary recap!

Write the following numbers in binary:

72, 255, 59, 91, 193, 0

Write the following numbers in decimal:

```
00011011
00001110
11011000
11111110
```

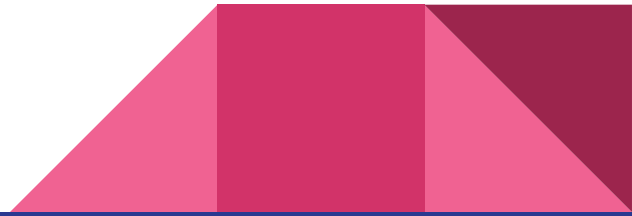


XOR

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Practice with XOR

- Get in teams of 2
- Each of you pick an 8 bit number
- XOR the two numbers
- Compare answers



One Time Pad - Encryption

Message: BEEPBOOP

ASCII encoding: 01000010 01000101 01000101 01010000 01000010 01001111 01001111 01010000

Key (secret, random): 00111001 00010000 10111001 00101101 10100000 11100110 01010110 01100100

XOR

Ciphertext: 01111011 01010101 11111100 01111101 11100010 10111100 01100100 00110100

Decoded ciphertext: {Uⁿ}Γ╝d4

0⊕0=0
0⊕1=1
1⊕0=1
1⊕1=0

Without knowledge of the key, it is **impossible** for an adversary to extract the message!

One Time Pad - Decryption

Do the same operation to the ciphertext to get the message back.

Ciphertext: {Uⁿ}Γ╝d4

ASCII encoding: 01111011010101011111110001111101111000101011110001100100000110100

Key (secret, random): 00111001000100001011100100101101101000001111001100101011011001000

XOR

Message: 01000010010001010100010101010000010000100100111101001111010100000

Decoded message: BEEPBOOP

0⊕0=0
0⊕1=1
1⊕0=1
1⊕1=0

One Time Pad activity

- Pick a 4 letter word.
- Convert each of the characters to an Ascii number.
- Convert the Ascii number to binary.
- Choose a random key which is equal to the length of your binary numbers
- XOR them
- Give your Ciphertext and Key to another person

About OTP

- Easy to implement/ compute (Encrypt and Decrypt are the same operation!)
- Computer can easily compute XOR.
- Unbreakable if the key is truly random and not known by the attacker.
- The only cipher that has perfect confidentiality.

Any problems with OTP?

Problems with the OTP

In order to share a secret message, you must first share a secret key. How do you share this key in the first place?

Key must be random.

Don’t know if a message is legitimate before decoding it.

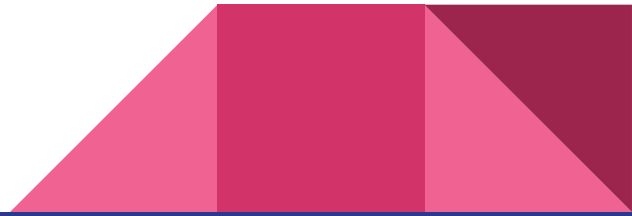
Key can only be used once.

Computer and randomness.

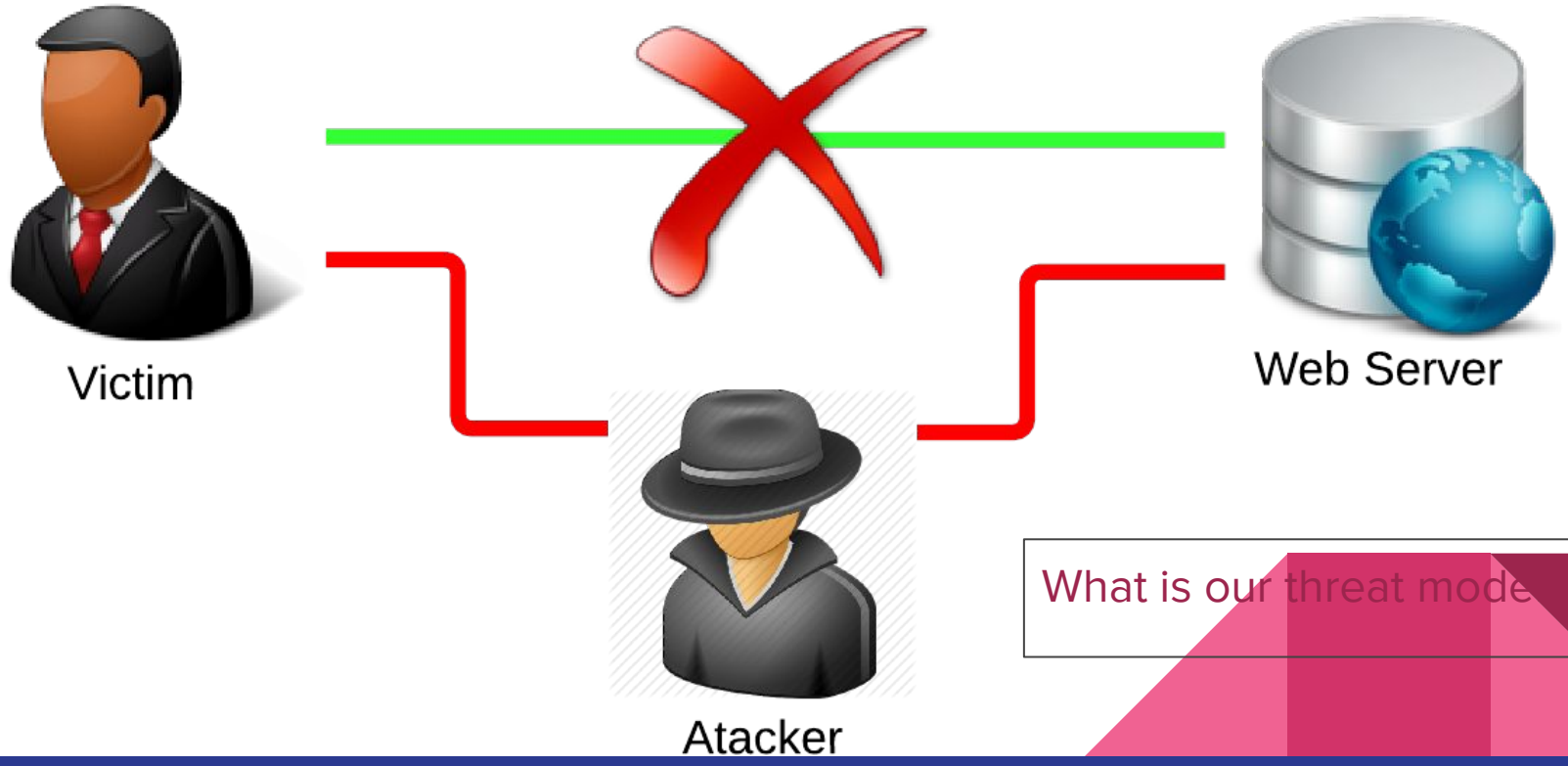
- Computers are bad at generating randoms
- Designed to give you accurate results
- It is supposed to eliminate randomness
- Computer functions are pseudorandom.

https://www.youtube.com/watch?v=9rIy0xY99a0

Integrity of One Time Pad



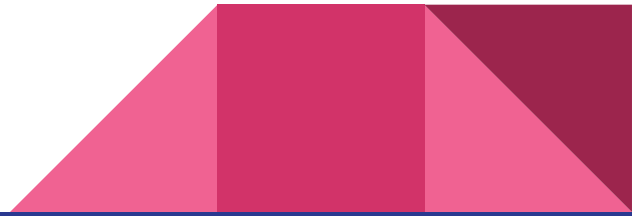
Man-in-the-middle



What is our threat mode

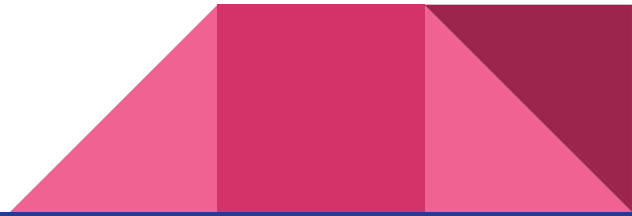
Integrity of One Time Pad

- It is very vulnerable to tampering.
- Alice is going to send Bob either 1 or 0, encrypted using OTP.
  - The adversary can just flip the bit in the ciphertext.
- Alice wants to send withdraw $1000 to the Bank, encrypted using OTP.
  - The adversary can just flip the bit again so Alice will never gets the right amount.



Key only use once

- It becomes Two Time Pad if you use the key twice.
- You can actually completely change the message if the key is used twice



Exercise Two Time Pad

Directions on worksheet.