Ethical Student Hackers

Cryptography

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at **shefesh.com/conduct**

What is Cryptography?

Cryptography is the art of writing secrets, it is a way to transfer information between different parties without directly disclosing what that information is.

Cryptography can broadly be seen as:

- Write a message
- Encrypt that message to hide its meaning
- Send that encoded message to someone
- Decrypt that message using a key or some complicated maths
- Read the original message

A key part of cryptography is that only people with “permission” can read that message.

A Brief History

Cryptography is derived from the Greek *kryptos* (hidden) + *graphien* (to write)

Early Uses:

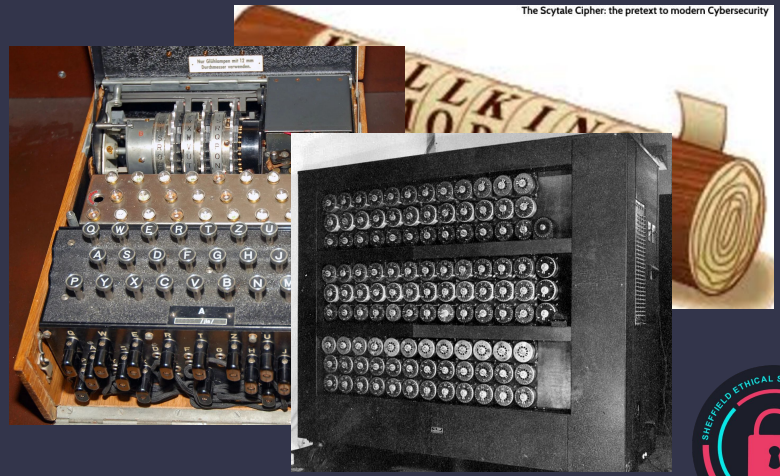
Sparta - Scytale Cipher, military transposition cipher using a rod and parchment strips
Julius Caesar - Caesar Cipher (unsurprisingly), shift substitution cipher for military comms

Medieval to Renaissance Period:

Arab Scholars (9th Century): Frequency Analysis
Leon Battista Alberti (1467): Polyalphabetic Ciphers
Vigenere Cipher (16th Century): Considered Unbreakable

Modern Day:

Enigma Machine: Broken using Bombe
RSA, AES, Diffie-Hellman
Quantum Cryptography



Cryptography Ciphers

A cipher is a method of writing these secret messages, you can pass your message into the cipher and get an output that is your secret, unreadable, message.

There are some key groups that ciphers and cryptographic algorithms can be split into:

- Monoalphabetic Substitution
- Polyalphabetic Substitution
- Mechanical
- Key-based Encryption
- Post-Quantum

Monoalphabetic Substitution

Monoalphabetic substitution ciphers encrypt messages by swapping letters for symbols according to a specified table, or sequence.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
QWERTYUIOPASDFGHJKLZXCVBNM

CIPHER -> EOHITK
```

Each letter is always mapped to the same letter in these types of ciphers. For example, if the letter C in your message is mapped to a G, every other C will also be mapped to a G.

A common example of one of these types of cipher is the Caesar Cipher.

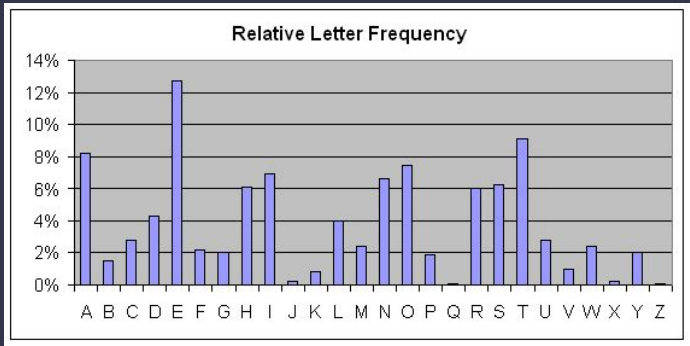
These ciphers can be additive/subtractive, multiplicative, or random assignment.

Frequency Analysis

Monoalphabetic substitution is very insecure and can easily be broken using frequency analysis.

Frequency analysis is a method we can use to see how often certain letters and words appear in an encrypted message.

For instance, if the letter P appeared more commonly than any other letter, it would be an accurate assumption that it would map to a commonly used letter, like the vowels.



There are a bunch of tools online for this, my favourite is: https://www.101computing.net/frequency-analysis/

Task #1

Easy:

YNKLLOKRJ KZNOIGR NGIQKXY

Medium:

eymqzymrhwynqkhsffmnnknoknbzsaoc

Hard:

YNC VUG LF GPJ UFHPNCGJB TNHXDNGJCA VY GPJ UFYNAPLVFNTWJ JFB VY GPJ DJAGJCF AELCNW NCR VY GPJ MNWNQZ WLJA N ARNWW UFCJMNCBJB ZJWWVD AUF.

Hint: Try to use frequency analysis

Polyalphabetic Substitution

Polyalphabetic substitution ciphers are similar to Monoalphabetic substitution ciphers, they also swap letters but do not directly map in a 1-to-1 relationship.

Monoalphabetic:
A always maps to G
Polyalphabetic:
A could map to G or S or even A

Because the frequency of letters can be different now, this protects these ciphers against frequency analysis.

minimum → ozlxfis
Note: M maps to o, f and s

A common example of one of these types of cipher is the Vigenère Cipher.

Vigenere Cipher

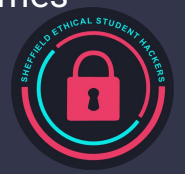
Combination of Caesar shift but combined with a keyword, the length of this keyword determines the number of different encryptions that are applied.

If the keyword is 5 characters long, the plaintext is split into 5 subtexts, with a different shift being applied to each one depending on the value of the corresponding letter in the keyword.

```
Keyword:    MATHMATHMATH MA THMAT HMAT
Plaintext:  CRYPTOGRAPHY IS SUPER COOL
Ciphertext: ORRWFOZYMPAF US LBBEK JAOE
```

Very difficult to brute force as each letter can be encoded to 26 different letters. Heavily dependant on the keyword so each message can be encoded in 26^(length of keyword) ways.

Main weakness is the repeating nature of the key, if the length of the key is guessed the cipher becomes smaller caesar ciphers.



Task #2

All of these ciphers are Vigenère Ciphers

Easy:

Zhgpmigvk

Key: Hack

Medium:

Eo Vhxj si Kxgaj. Seln Fue.

Key: Rapture

Hard:

N nenxf si trj miri gvwt

Vnbi ny tei efji aac

Yf gadhy xhor zw mi wvel djjx

Ty yieix yyim sx dc ckzji

I gncp tbfmil khissc yyi lksu

Wekwtlixl wer ksu ainj

Kiamm Gskéwte xo esuircyrrd

Dmv togji xhky'j mncnui

Key Length: 5

Mechanical

Mechanical cryptography uses physical machines to automate substitutions and transpositions.

The most famous example of this is the Enigma machines used by Germany during WWII.

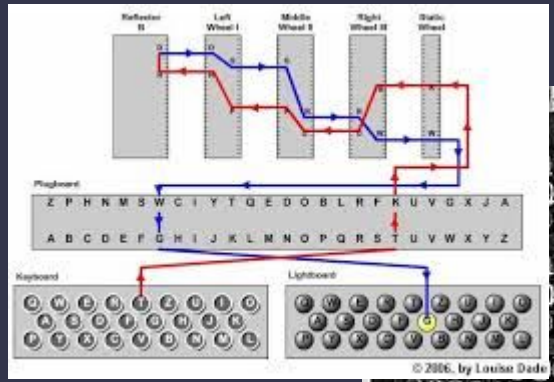
The Enigma was based around a set rotors to create a polyalphabetic substitution, with each key press the rotors would change position.

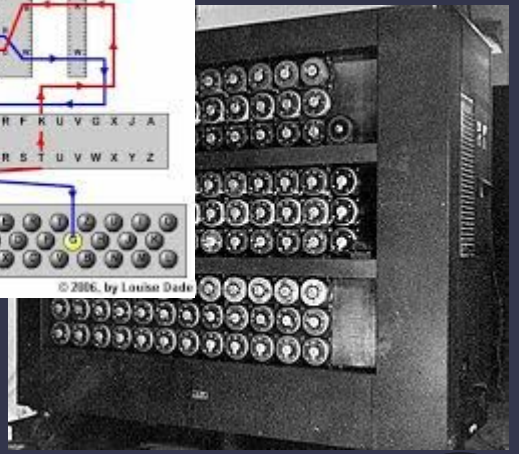
An older method of mechanical cryptography is the Scytale which was used in the 7th century BC, using a cylinder with a parchment strip.

Enigma Machine

The Enigma Machine was used in WWII to communicate between Germany Army, it was famously cracked by Alan Turing using The Bombe.

The way the machine worked was a user would set up an initial configuration (has to be the same encoding and decoding) and use the keyboard to input.





The pegboard, rotors, rings and reflectors are what is configured by the user.

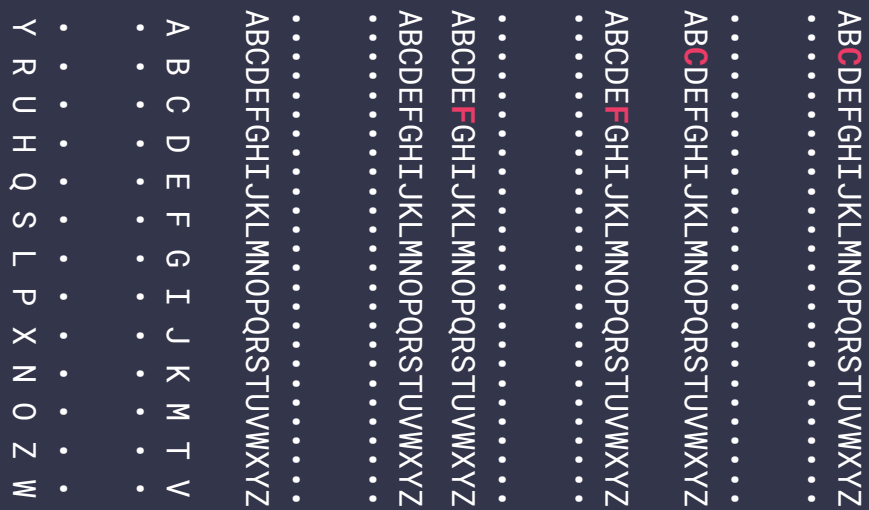
Inputs will follow this pipeline:
Keyboard -> Pegboard -> RIII -> RII -> RI -> Reflector -> RI -> RII -> RIII -> Pegboard -> Lightboard

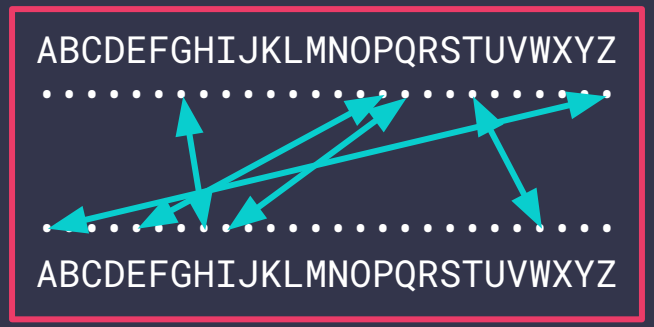
The rotors rotate at certain inputs which scrambles the message.

Task #3

Easy:
Decode CSKD

Hard:
Decode BMKRWZ





Feedback

Please leave your feedback :) We want to know what we can do to improve.

Please leave constructive and honest feedback only.

https://forms.gle/VTYd74K5BHqbC7F68

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

The week after that

And the week after that

And the week after that

And the week after that

Any Questions?

www.shefesh.com

Thanks for coming!