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

Is it a science, an art or both?

“Technologies primarily based on maths and computer science for protecting information so that it is only accessible to authorised recipients.” - National Cyber Security Centre

It can be very performative though -

The zodiac killer - two ciphers, one easy one near impossible (solved in 2020)

Kryptos - 5 ciphers, 3 solved, one unsolved and one to be discovered

SO WHICH IS IT

Read more: https://www.britannica.com/topic/philosophy-of-art

What are our goals?

CIA

Confidentiality • Prevent information disclosure to unauthorised parties

Integrity • Prevent information modification to unauthorised parties

Availability • Ensure information is accessible to authorised parties

How does it affect you?

WOOCLAPPPP 👏👏👏

ZMOIDJ

History of Cryptography

1900 BC - Inside the tomb of Khnumhotep II there are non standard hieroglyphs believed to be the first use of cryptography

600BC - Spartans used scytale devices to send secret messages during battle, This is a leather strap wrapped around a wooden rod. Letters on the leather strip are meaningless when unwrapped.

Question: *What is the 'key'* of a scytale device?

60BC - Julius caesar would shift characters 3 along in the alphabet during private correspondence. A -> D. This lead to the naming of the caesar cipher which is a simple substitution cipher. (more in a sec)

Give it a Go: *Shvwqoz Voqysfg wg hvs psgh!*

Types of Cryptography

Classical:

- Substitution: Substitute character(s) for other characters - Caesar, Vigenère or Playfair
- Transposition: Rearrange the order of characters within a plaintext - Rail fence or Columnar

Question - *Do you think these types of ciphers are still used?*

Plantext?
Text before encryption (ciphertext)

Modern:

- Symmetric key Encryption: DES, AES, OTP
- Asymmetric key Encryption: RSA, Diffie Hellman, Elliptic Curve Cryptography

Future:

- Post quantum cryptography??

How cryptography works

More or less all cryptographic systems used in applications today are made up of basic components or *primitives*

Substitution-box (S-box)

Takes an n-bit input and outputs an m-bit output using a simple lookup table

Permutation-box (P-box)

Takes an n-bit input, mixes up those bits and then produces an n-bit output

These are then extended and used to create other primitives e.g Expansion P box, compression P-box

Stream vs Block ciphers

Stream cipher

Each bit is individually encrypted by the key.

Simple implementation of this is the **One Time Pad** (OTP) - each plaintext bit is XORed with a key bit

Where the sender and receiver both hold the key this can create perfect encryption.
-> even with unlimited computation no information about the plaintext can be retrieved

Question: *Can anyone tell me why a key could only be used once?*

Block cipher

Plaintext gets encrypted in blocks of size N using key K of size k.

Normal N, K values DES, N, K = 64, 56. AES, N, K = 128, 128

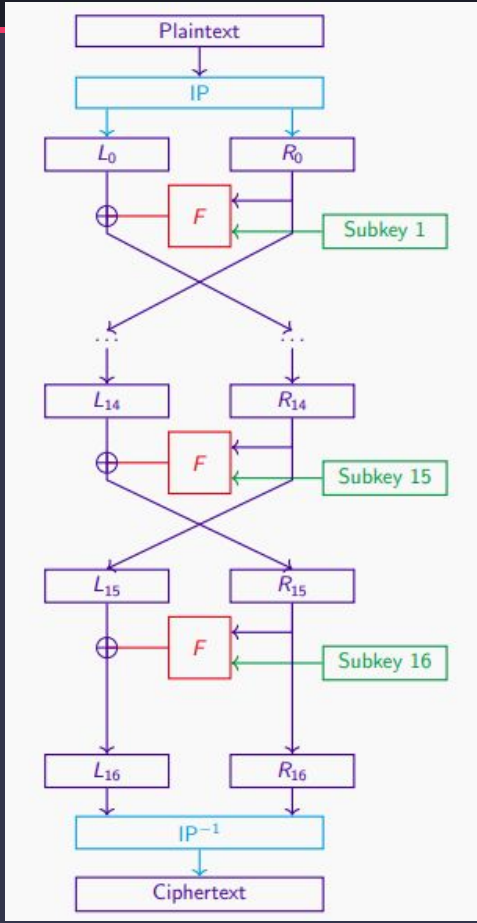
CHALLENGE :

Try designing your own block cipher!!

Can work together if you like and Im gonna ask for your suggestions

Now time to touch the surface on some very important systems which you probably use on a **daily basis**

Data Encryption Standard (DES)



Notes

Initial Permutation (IP), also splits the text into two parts

Uses A Feistel Cipher (F) -

Complex combination of Compression, S-boxes and P-boxes

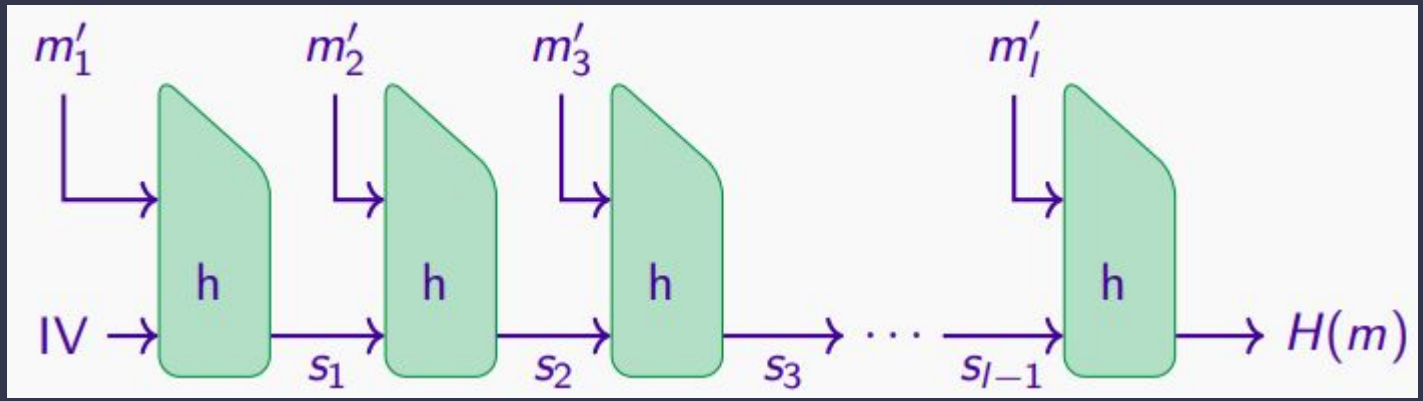
The 56 bit key is rotated around to create unique subkeys for each round.

Hashing

Takes any sized input and outputs a fixed length string. Think of any issues with this?

Based off of compression function **h()** (which is based off of block ciphers - remember how I said cryptography is built on primitives?) **h() : {0,1}length K+N -> {0,1)length N**

1. Pad the plaintext using a padding scheme (ANOTHER important primitive)
2. Break up m' = pad(m) into blocks length K
3. Apply this:



Diffie-Hellman key exchange

Alice Bob

1. Pick a large prime number p and primitive (:D) root g
2. Alice and Bob then each select a random number a and b
3. Create their public keys e.g A = g^a mod p
4. Give their public keys to the other
5. Compute the other public key with their own private key
   S_A = B^a mod p, S_B = A^b mod p

S_A = S_B due to modular arithmetic and they now both have a symmetric key

Noticed something? - this in itself is a public key cryptographic system

RSA

https://www.youtube.com/watch?v=wcbH4t5SJpg

I don’t understand it amazingly so this guy gonna help me out here

Resources

Fabulous website where you can learn more and apply some of the things we have learnt today :D

https://cryptohack.org/

Learn about cryptanalysis (the science of analysing and breaking down cryptographic functions):

https://www.geeksforgeeks.org/cryptanalysis-and-types-of-attacks/

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

AGM

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Next week: Docker

The week after that: Easter

Any Questions?

www.shefesh.com

Thanks for coming!