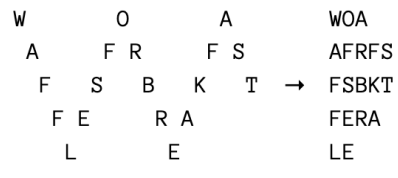
Unit #1

Cryptography: Encryption/Decryption

- **Ciphers** are algorithms used to encrypt and decode messages.

<table>
<tr><td>Encryption methods</td><td colspan="2"></td></tr>
<tr><td rowspan="4">Symmetric</td><td colspan="2">● The usage of one single private key to encrypt and decrypt data.
● It requires higher security since it uses one key.
● Widely used today.
● Comes in two forms: stream ciphers (encrypts bit by bit) and block ciphers (Data is transformed into blocks of data and is encrypted block by block).
● Uses two cipher techniques: substitution and transposition.
● TLS/SSL Protocol: TLS handshake generates symmetric encryption keys for the client and server.</td></tr>
<tr><td colspan="2">Types of symmetric ciphers</td></tr>
<tr><td>Substitution</td><td>● Substitutes different letters, numbers, or other characters for each character in the original text.

Examples of substitution ciphers:
1. Monoalphabetic cipher: letters of plaintext have a one-to-one relationship with letters of ciphertext.
● Caesar cipher: a simple shifting method where letters are shifted by some fixed number. Eg. a shift of 2 means A encodes as C.
2. Polyalphabetic cipher: a single plaintext letter has multiple substitution alphabets.
● Vingenère cipher: uses a keyword used on the Vingenère table to encrypt and decrypt.
3. Base64
● Encrypted texts end with a ‘==’.
4. Playfair cipher
5. Hill cipher
6. One-time pad
7. Advanced Encryption Standard (AES): Currently one of the most widely used symmetric algorithms.
8. Blowfish (64-bit)/Twofish (128-bit): Alternative block ciphers to DES.</td></tr>
<tr><td>Transposition</td><td>● Scrambles the position of characters without changing</td></tr>
</table>

		the characters themselves. **Examples of transposition ciphers:** 1. **Rail fence cipher:** rearranges text in a “wave” pattern and condenses the letters on the same rows.  = WOA AFRFS FSBKT FERA LE 2. **Row column transposition**
Asymmetric	● Uses a pair of a public key (encrypting) and a private key (decrypting). ● Only authorized users have access to the private key but the public key is accessible by anyone. ● Widely used today. ● Uses mathematical algorithms to encrypt data. **Examples of asymmetric algorithms:** 1. **Rivest Shamir Adleman (RSA)** 2. **Digital Signature Standard (DSS)** 3. **TLS/SSL Protocol:** Uses asymmetric encryption to establish a secure client-server session.	

https://crypto.stackexchange.com/questions/43028/is-a-transposition-cipher-categorized-as-asymmetric-algorithm

- **Magic number -** the first bits of a file that uniquely identify the file type.
  - https://gist.github.com/leommoore/f9e57ba2aa4bf197ebc5
- **Hashing -** a one-way mathematical function that turns data into a string of nondescript text that cannot be reversed or decoded.
  - It is not encryption, that’s why it can’t be reversed.
- **Salting -** a random string that is added to a password before it’s hashed. This helps enhance the security.
  - The salt should be stored with the hash.

Lab

1. Terng wbo qrpbqvat lbhe svefg pvcure! → Great job decoding your first cipher! **[ROT13]**
   - ROT13 is a variant of Caesar cipher.

2. !#CTOAHDPE#! → CODEPATH **[Rail fence].** Acx'vt dhppu dqpzbui! Yhie im br! → You're doing amazing! Keep it up! **[Vingenère]**
   - (had to decrypt the key using rail fence and then decrypt the message with the key)

- For rail fence decryption, non-alphabetical characters are ignored because the algorithm only works with letters.

3. Ijhtinsl rjxxfljx nx kzs, gzy bmfy jqxj hfs bj it?! → Decoding messages is fun, but what else can we do?! **[ROT13 but shift of 22]**

4. The file has ‘ab 20 10 5d’ as the magic number. However, the file type is .png and .png’s magic number is ‘89 50 4e 47’, so no image appeared. In the input, i had to change the magic number to the correct one, then convert it from hex, and then render the image to see it.

5. The .png shows a black rectangle when rendered. I adjusted the lightness of the photo to reveal the hidden message ‘I’m impressed!’.

6. ***Provided key:*** 8621ffdbc5698829397d97767ac13db3 and ***provided message:*** Qfw ech'uv rkoqb wox huh gruxrfk! I had to use Crack Station to crack the hash which resulted in ‘dragon’. Qfw ech'uv rkoqb wox huh gruxrfk! → Now you're ready for the project! **[Vingenère]**

Project

Trivia

1. This aspect of the CIA triad is about ensuring that information is not altered accidentally or by entities unauthorized to make alterations. **Integrity**
2. According to CyberSeek, which state has the highest numbers of cybersecurity job openings? **Virginia**
3. This kind of malicious software will encrypt the files on your harddrive and only provide a decryption key when you pay hackers a hefty fee, usually in cryptocurrency. **Ransomware**

Reconnaissance

4. What's Next? 11,185,272 **The second largest prime number discovered by the GIMPS project.**
5. Can you find the flag in the README.txt? **flag{h3r3syerfl@g}**
6. What's the secret code?

Number of correct digits	Number of correct digits that are correctly placed
4	1
3	3
1	0
2	0
2	1

3	2	8	5	1
9	4	8	1	5
8	0	1	9	6
7	8	9	5	1
7	0	2	3	6

Inspired by: IEEE PuZzLeRs

What's the code?

Cryptography

7. Qeb mxpptloa fp MibxpbZexkdbJb → **The password is PleaseChangeMe** [ROT13 with shift 3)
8. aXRnZXRzaGFyZGVyZnJvbWhlcmU= → **itgetsharderfromhere** [Base64]
9. The key has been encoded TWICE! ***Message:*** JYWMEIDVRTTYDOZPEDSUGQ ***Key:*** POELR → **HAVINGFUNCRACKINGCODES** [For the key: ROT13 + Caesar, For the message: Vigenère]
10. AAAAA AAAAB BAAAA AAAAA AAABA AAAAA AAABB AAAAA AAAAB BAAAA AAAAA → **ABRACADABRA** [Bacon cipher]
11. Someone is trying to hide information in the metadata. → **flag{h1ding_in_plane_s1ght}**