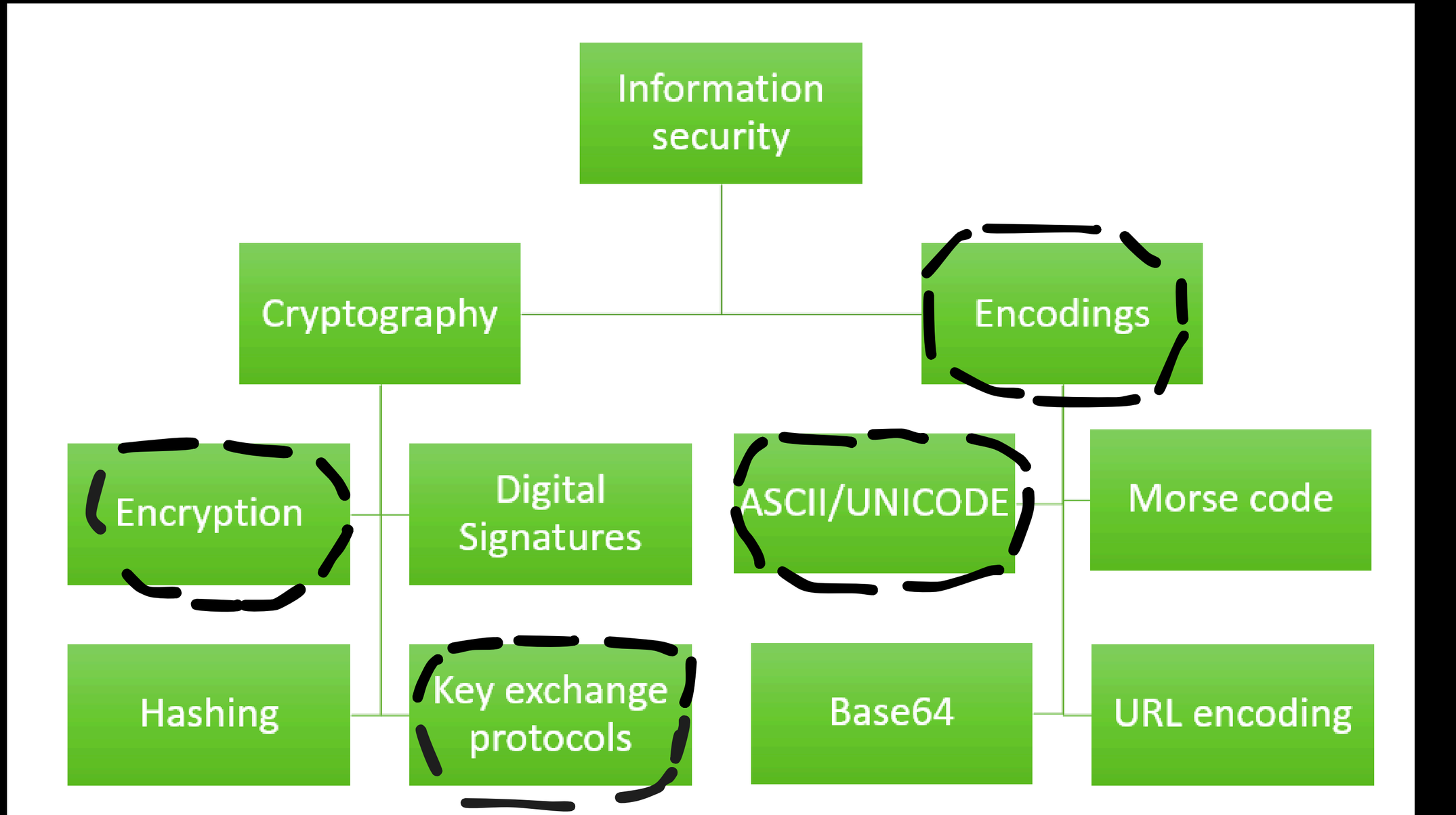
Updates - Submissions + Challenge cards
Week ahead and how people need to get familiar


Information security
Cryptography
Encodings
Encryption
Digital Signatures
ASCII/UNICODE
Morse code
Hashing
Key exchange protocols
Base64
URL encoding

OUR FOCUS WITHIN INFO SECURITY

CRYPTOGRAPHY

The science of securing communication through techniques like encryption, hashing, and digital signatures.

ENCRYPTION

A method within cryptography that transforms readable data (plaintext) into unreadable data (ciphertext) using a key, to ensure confidentiality.

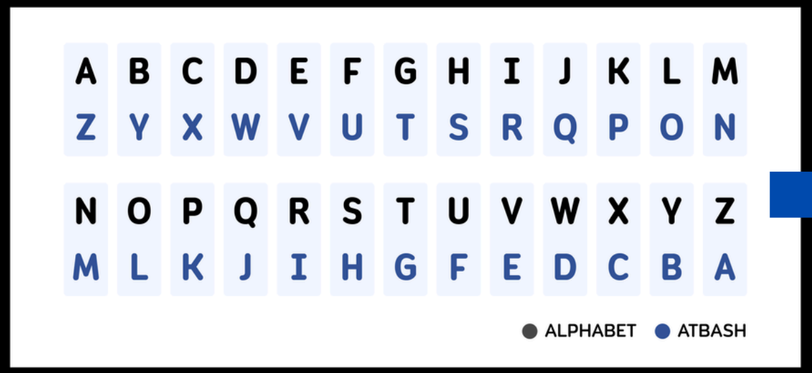
ENCODINGS

The process of converting data into a different format for compatibility or transmission, using publicly known rules — not meant for secrecy.

ENCODINGS

Below are historical ciphers that once served encryption purposes, but no longer meet modern definitions due to lack of a secret key and low security.

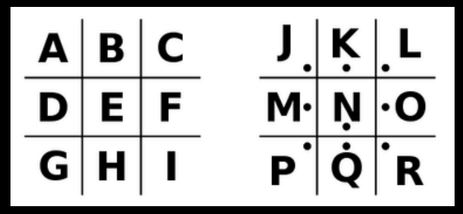
ATBASH CIPHER

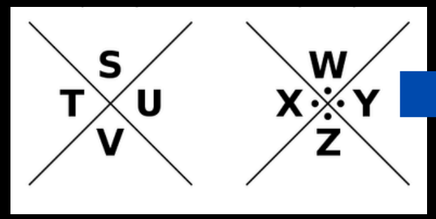


Each letter in the alphabet is mapped to its reverse counterpart (A ⇔ Z, B ⇔ Y, C ⇔ X, etc.).

Decipher:
1. FNYIVOOZ
2. NZTRX

PIGPEN CIPHER



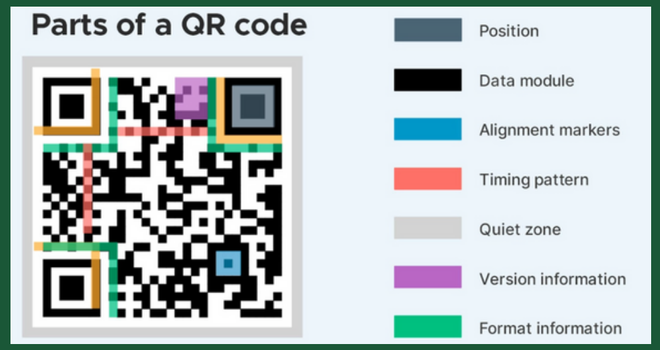


Pigpen Cipher is a geometrical monoalphabetic substitution cipher.

Decipher:

Any 1-1 bijective mapping (uniquely reversible) is a valid form of encoding data.

QR CODES



Make your own!

Remember: You should always be able to retrieve the original data uniquely.

ASCII ENCODING

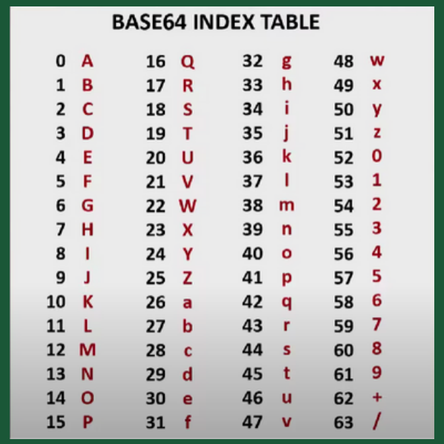
A → 65

B-> 66

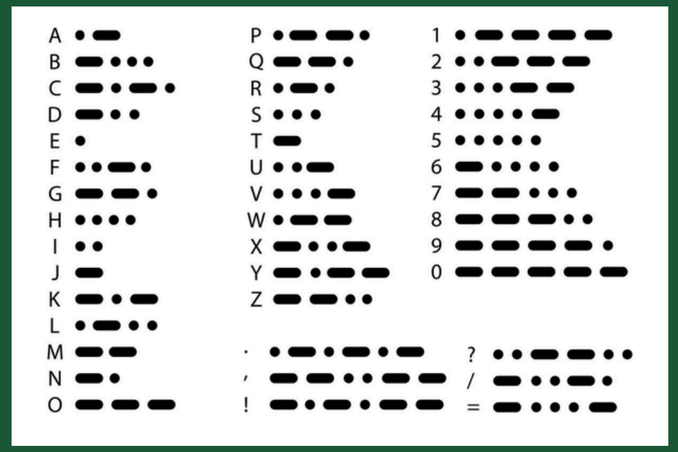
C-> 67

...

BASE64



MORSE CODE



ATBASH, PIGPEN

ENCRYPTION TECHNIQUES

SYMMETRIC FROM A → B

PLAIN TEXT OF A

PLAIN TEXT DECRYPTED BY B

ENCYRPT KEY - SHARED

CIPHER TEXT

DECRYPT KEY - SHARED

ASYMMETRIC FROM A → B

PLAIN TEXT OF A

PUBLIC KEY OF B

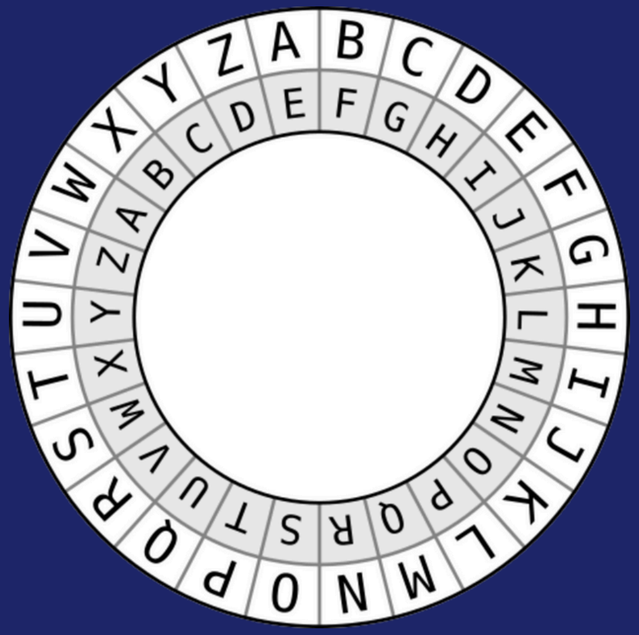
CIPHER TEXT

PLAIN TEXT DECRYPTED BY B

PRIVATE KEY OF B

SYMMETRIC ENCRYPTION TECHNIQUES

Caesar Cipher *SHIFT KEY = 4*



Wrap the alphabet around in a circle and push each letter ahead by shift key

Examples:

A → E

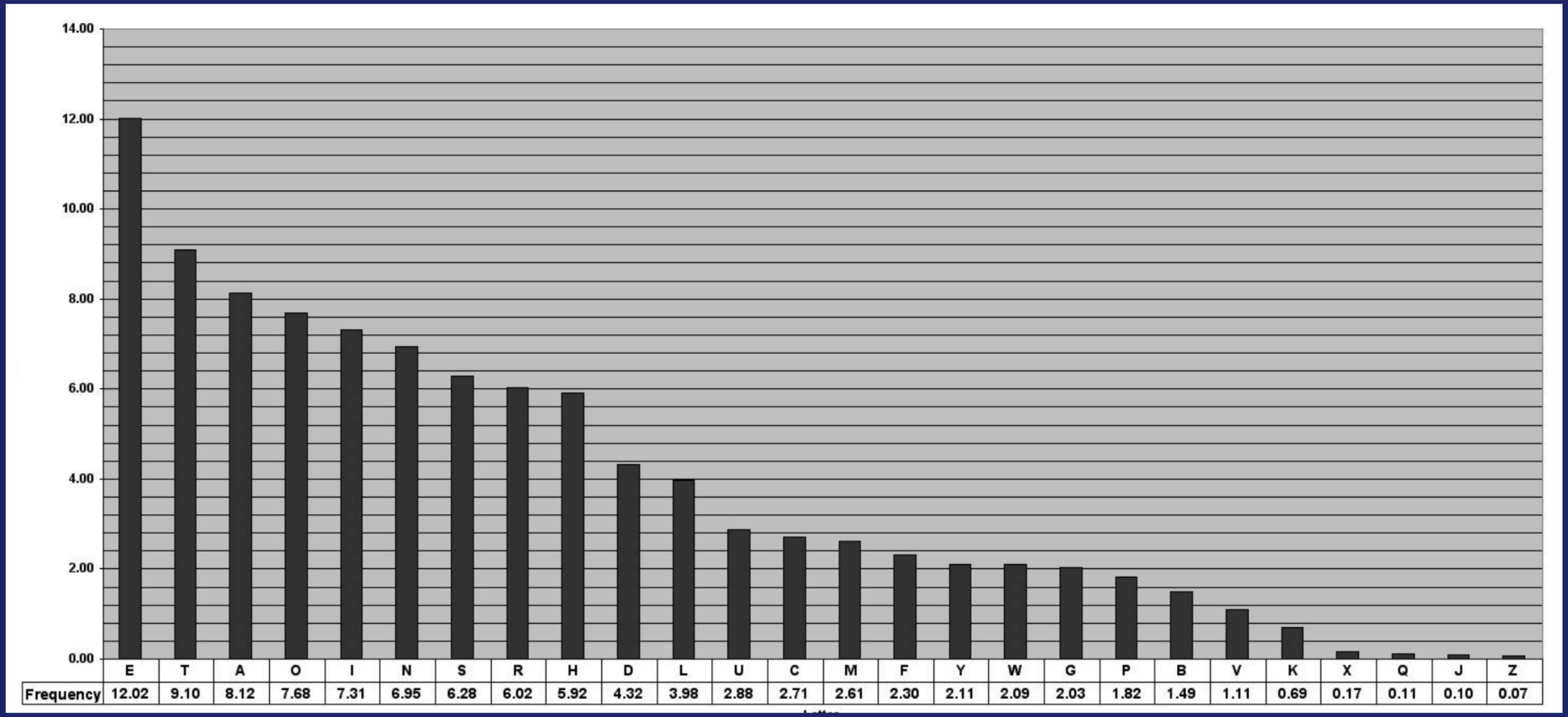
B → F

Z → D (due to the wrap around)

THINK!! 💡

What would happen if we have a negative shift key? If you could make certain assumptions of the plain-text, can you decrypt the message without knowing the key?

Hint: How can we use the frequency of letters in the English Language?



	E	T	A	O	I	N	S	R	H	D	L	U	C	M	F	Y	W	G	P	B	V	K	X	Q	J	Z
Frequency	12.02	9.10	8.12	7.68	7.31	6.95	6.28	6.02	5.92	4.32	3.98	2.88	2.71	2.61	2.30	2.11	2.09	2.03	1.82	1.49	1.11	0.69	0.17	0.11	0.10	0.07

VIGENERE CIPHER

- Key (K) : FRINGE
- Plain text(P): get all soldier a meal.
- Cipher text(C):

Note: This Vigenere is P[i] + K[i]

K	F	R	I	N	G	E	F	R	I	N	G	E	F	R	I	N	G	E
P	g	e	t	a	l	l	s	o	l	d	i	e	r	a	m	e	a	l
C	M	W	C	O	S	Q	Y	G	U	R	P	J	X	S	V	S	H	Q

F S Y

How does Vigenère's use of multiple shifts change letter frequency patterns compared to Caesar's single shift, and why does that make it harder to break?


What aspects of symmetric encryption make it susceptible to attack?

Think:

How do the sender and receiver agree upon a shared key without a listening third party also knowing? (paint activity – explain clearly)

Think further:

Even if two people agree upon a secret shared key, is it possible for the passing message to be tampered with/be heard?

Think Further Still:

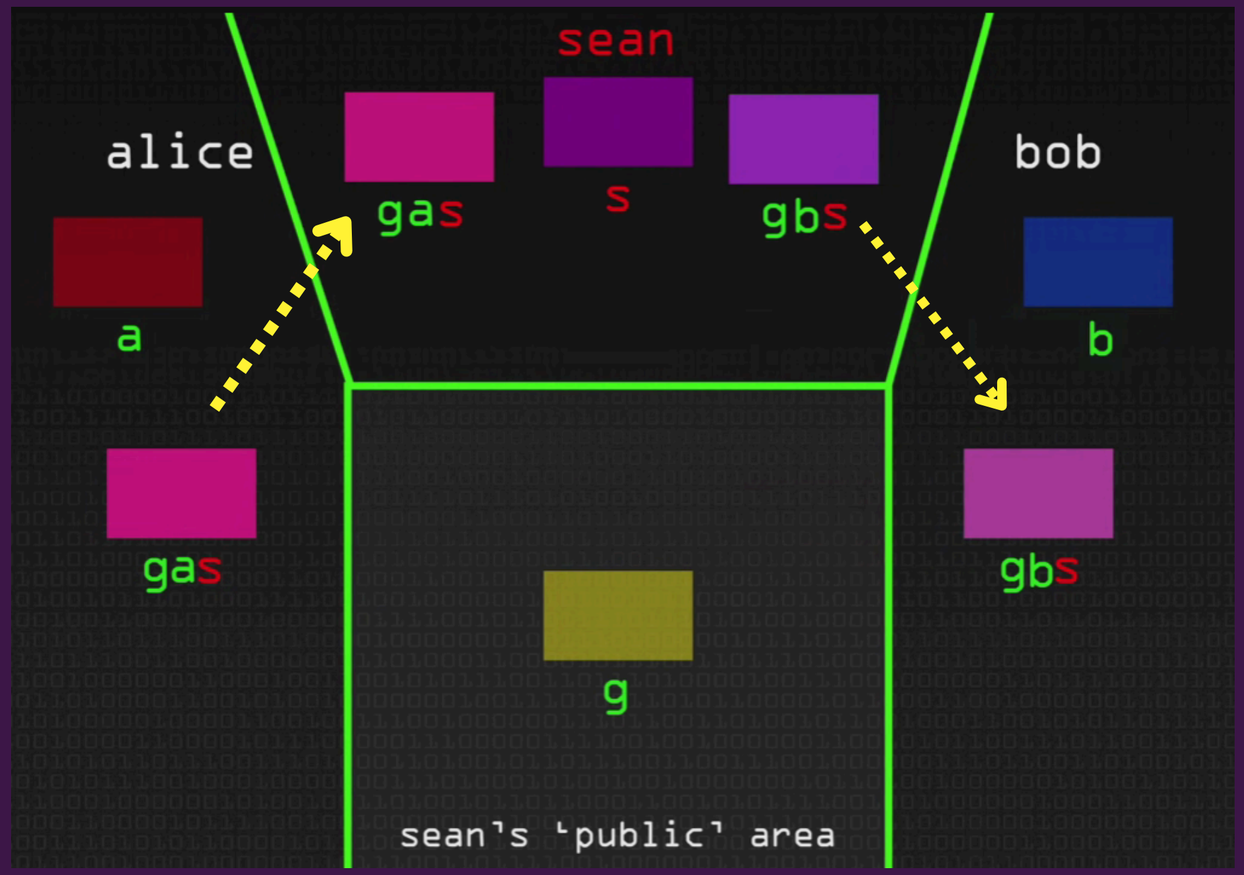
How can we resolve this situation?

Diffie-Hellman to get shared secret key

starting from 2: 47 till end Diffie-Hellman Key Exchange

Discrete Logarithm problem: it is difficult to know x after computing
$g^x \bmod n = m$ (this is the value sent across which can be int

Issue with Diffie Hellman Key Exchange



Sean acts as the middleman here and pretends to be Alice and Bob. He can overhear and even tamper with the conversations between them.

Need for identity proof
look into: digital signatures

ASYMMETRIC ENCRYPTION TECHNIQUES

https://www.youtube.com/watch?v=hm8s6FAc4pg&t=224s