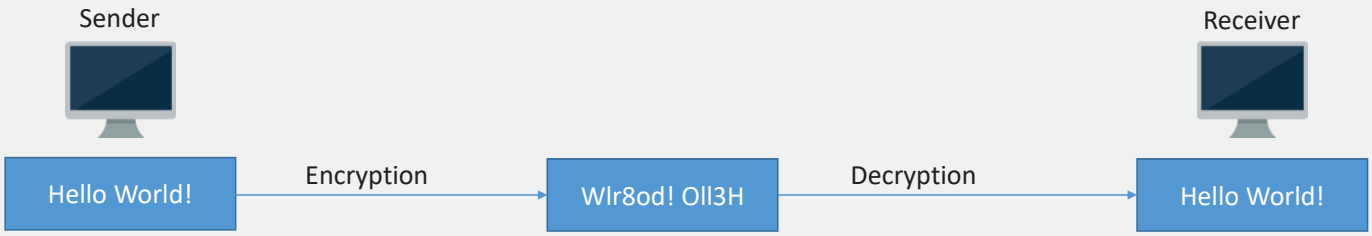
Encryption

Benny Ankri

What is 3|\|(rypt!0|\|?

- Encryption: The process of coding text
- Decryption: The process of decoding text
- A security method used to protect data
  - File/Programs on the computer
  - Files are stored on external media
  - Data being passed through the internet



Caesars's Chipper

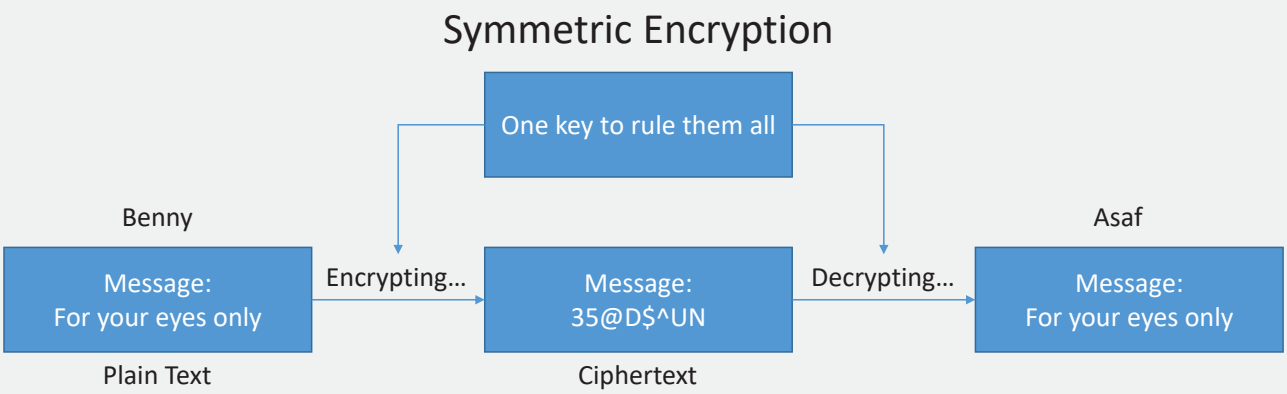
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Value 0

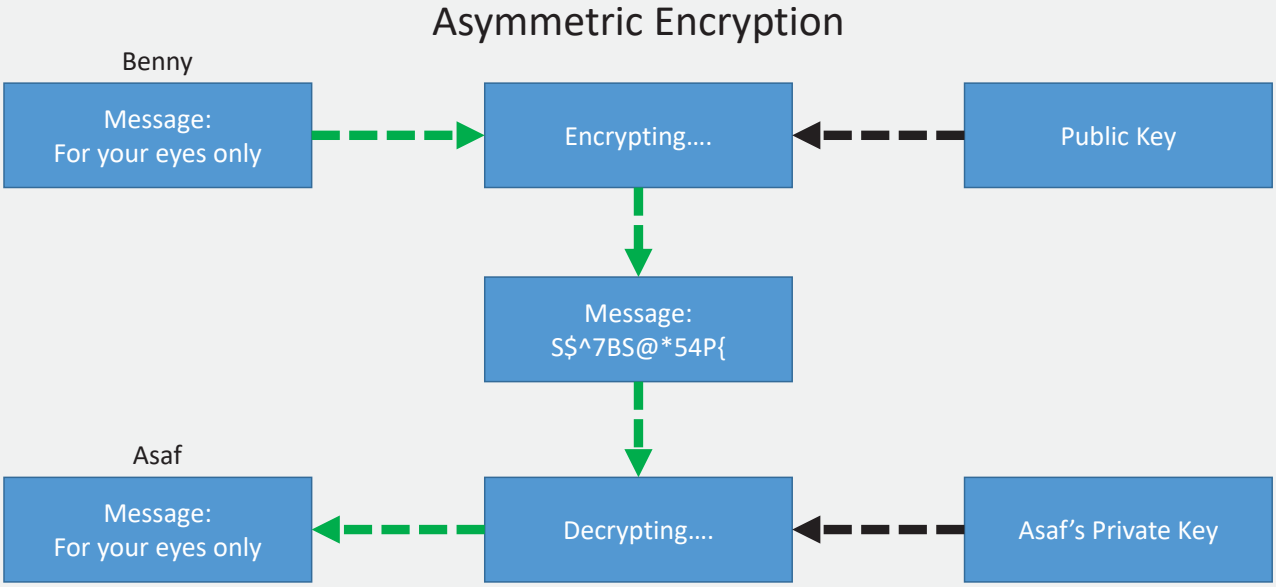
Categories of Cryptography

- Symmetric Encryption
- Asymmetric Encryption (Public Key Encryption)

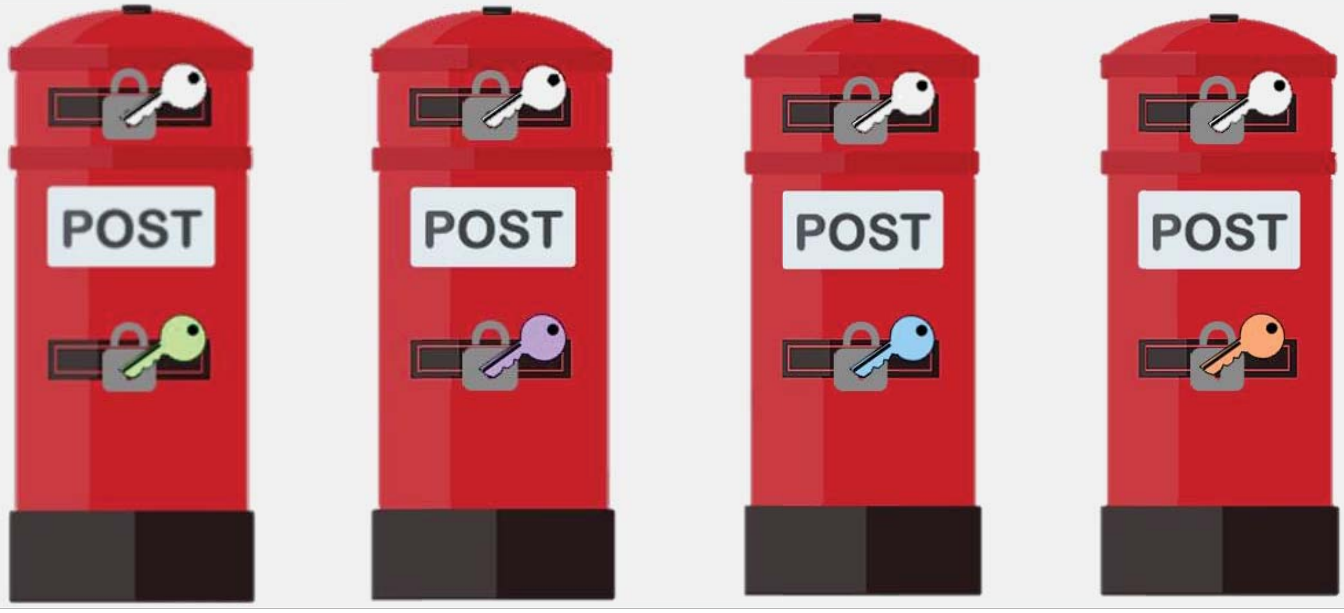
How does it work?



How does it work?

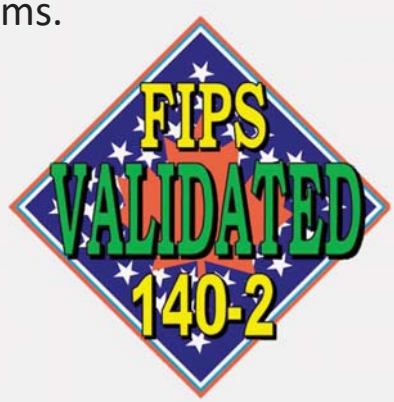


Example Asymmetric Encryption



Federal Information Processing Standards

- **Federal Information Processing Standards** (**FIPS**) are publicly announced standards developed by the United States federal government for use in computer systems.



Data Encryption Algorithm

	DES/3DES	AES
Developed	1977/1998	2000
Key Length	56 bits	128, 192, 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128 bits
Security	Proven inadequate	Considered secure
FIPS Compliance	Yes	Yes

Type of data

Types of Encryptions – Data at Rest

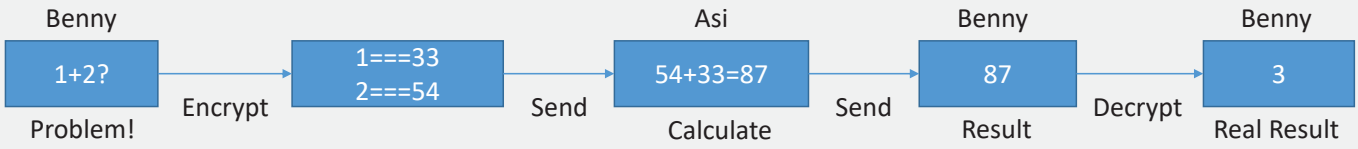
- File Based Encryption
- Full Disk Encryption
- Self Encrypted Drive

Types of Encryptions – Data at Motion

- HTTPS
- SSH
- SSL
- TLS
- FTPS
- VPN
- Encrypted VPN

Types of Encryptions – Data at Use

- HSM - Hardware Security Model
- TPM - Trusted Platform Module
- Homomorphic encryption



As Cory Doctorow said once…

"Why I love technology: if you used it right, it could give you power and privacy."