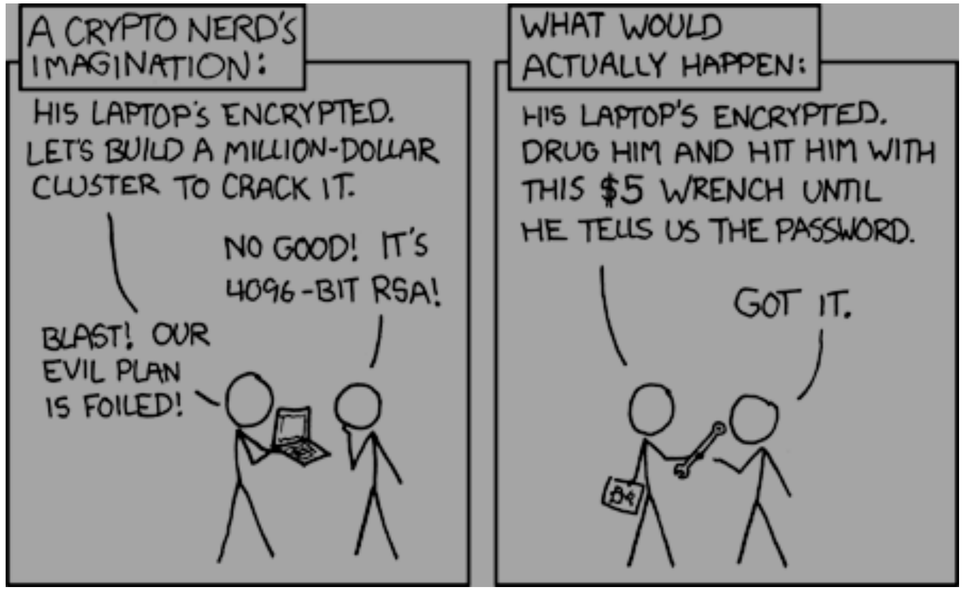
Cryptography



Agenda

- Review
- Dive into VI
- History of Cryptography (light)
- Symmetric vs Asymmetric Encryption
- Hands-on with Encryption
- Hashing and Digital Signatures
- Recap

Review

- What command would show the current directory I am in?
- What command allows me to change directories?
- What command shows the files in a directory?
- What command will show the contents of a file?
- Which command allows me to change the permissions of a file?
- What is the difference between the following two characters: > |
- Given the following command, what permissions does the owner have?
  - chmod 640
- What about the group?
- What about everyone else?

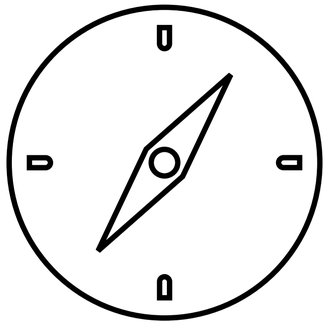
Intro to VI

- Open your VM!

What is Cryptography

- Definition: "Cryptography is the practice of developing and using coded algorithms to protect and obscure transmitted information so that it may only be read by those with the permission and ability to decrypt it. Put differently, cryptography obscures communications so that unauthorized parties are unable to access them." - IBM https://www.ibm.com/topics/cryptography

- Confidentiality - Ensure only those that *should* have access to data can see it
- Integrity - Ensure that data has not been modified by other parties



Where and How it is Used

- Below are some examples:
  - Storing secret information like passwords
  - Secure web browsing and transmission of information
  - Secure authentication - proving identities
  - Digital signatures - proving who people are or things have not been modified
  - Non repudiation - proving that this is from a person and they cannot deny

Key Terms

- Clear Text
  - The unencrypted text (e.g. "A dog")
- Cipher
  - The encrypted text (e.g., "<&a0B a")
- Encryption
  - The process of turning clear text into encrypted text
- Decryption
  - The process of turning encrypted text into clear text

Key Terms

- Key
  - What do I use to convert the plain text into encrypted text and vice versa
  - Do I use the same key for both encryption and decryption, or two separate keys
- Algorithm
  - What are the steps to turning encrypted text into clear text and vice versa
  - Determines how the key is used
- Encoding
  - Transforming data from one format to another
  - NOT encryption
  - https://www.base64encode.org/

History

- Caesar
  - One of the earlier ciphers
  - Substitution based cipher
  - One letter maps to another
- What does the following say?
  - ACGGJ
  - HELLO

Plaintext

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

Substitution

One-Time Pad

- Vernam Cipher
  - Shift plain text letters given a pad
  - Pad acts as a "key"

One-time pad

4	5	13	1	13
2	14	19	6	23
8	2	26	5	2
16	24	1	25	3
6	14	6	10	20

Plaintext	A	T	T	A	C	K	A	T	D	A	W	N
Shift	4	5	13	1	13	2	14	19	6	23	8	2
Substitution	E	Y	G	B	P	M	O	M	J	X	E	P

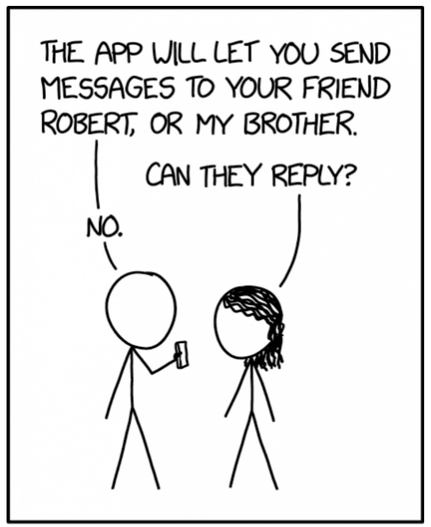
- Given the following message and one time pad, what does it say?
  - VXZNE
  - 3,4,5,10,6
  - STUDY

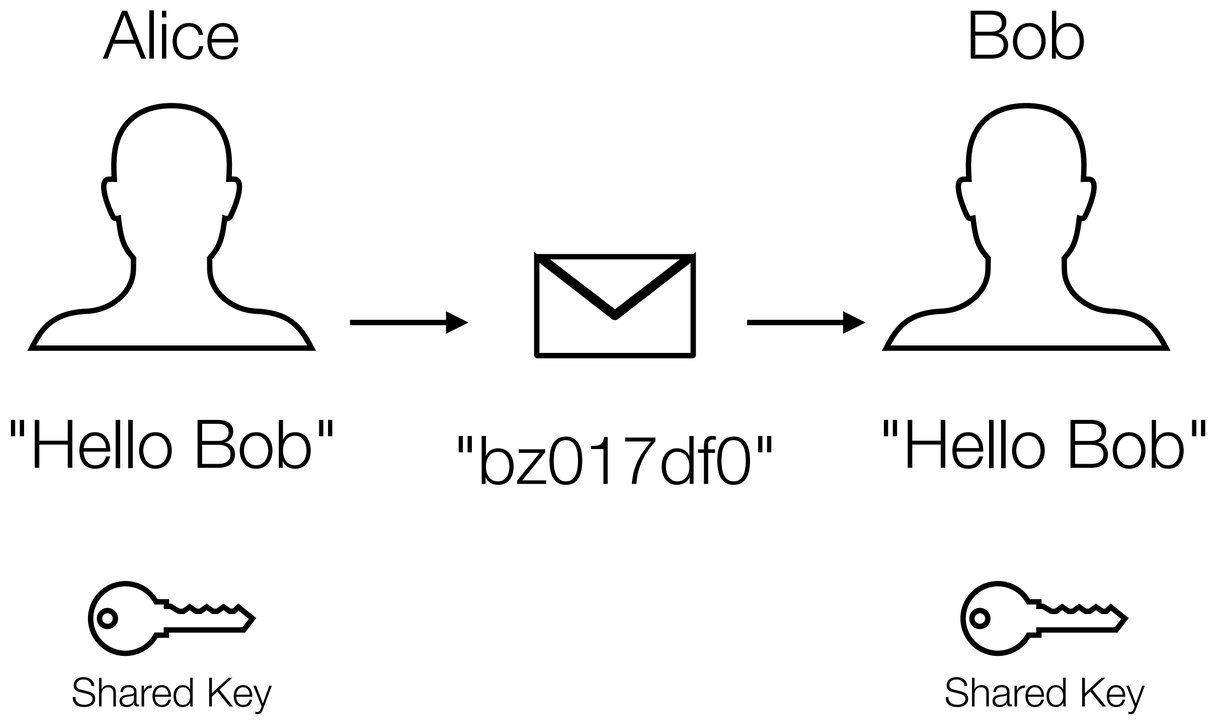
History - Enigma

- WW2 - Enigma used to transmit secret messages
- Alan Turing & Team at Bletchley Park
  - Created computer "The Bombe" to crack the enigma
  - Electromechanical machine
  - Information was powerful
- Popularized in movie "The Imitation Game"
  - Turing test (imitation game)
  - Computer seems to be a human

Symmetric Encryption

- The same key is used for both encryption and decryption
- Very fast compared to asymmetric
- Both parties must know key





Symmetric (contd)

- Popular Algorithms
  - DES / 3DES - Data Encryption Standard - Don't Use
  - Blowfish - Don't Use
  - RC4 - Don't Use
  - AES - Advanced Encryption Standard - Use (128, 192, 256 key sizes)
- Block vs Stream
  - Stream - Encrypt bits one bit at a time
  - Block - Take a set number of bits (more popular)
    - ECB - Electronic Code Book - Don't Use
    - CBC - Cipher Block Chaining (cannot run in parallel, can use)
    - GCM - Galois Counter Mode (can run in parallel, should use when possible)

"Encrypted" Image using ECB

Let's Try It Out!

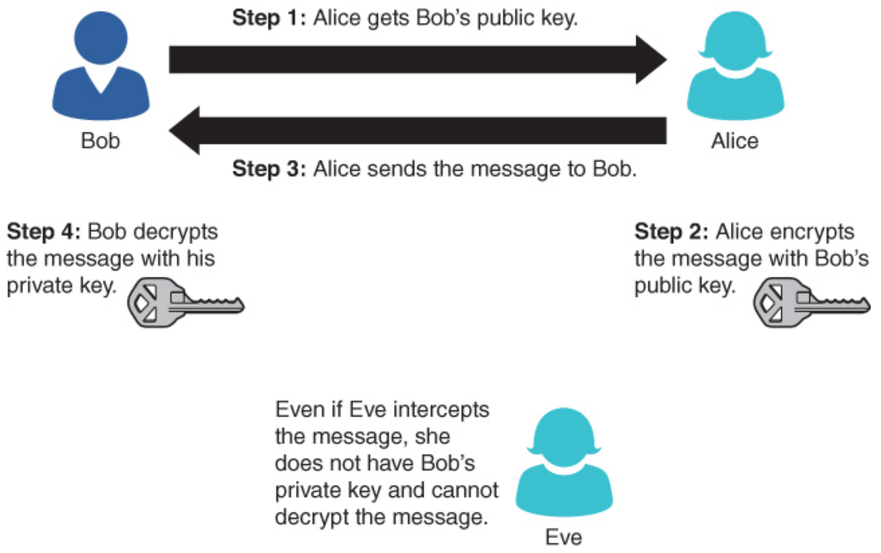
- Open your VM

Downside of Symmetric

- Really easy to do and very fast ... but
- What if you want to send a message to someone you don't know?
- How would you safely and securely get the key to them?
- What if you don't trust them?
- Then, do you create a separate key for each person you want to communicate with?

Asymmetric

- Two separate keys are used: public and private key
- Slower than symmetric and larger keys sizes
- But, it allows other people to send you message using your public key
  - No need to distribute key
- MUST keep private key safe



Asymmetric

- Popular Algorithms
  - RSA - Ron Rivest, Adi Shamir, and Len Adleman (Mathematician)
    - 1024, 2048, or 4096 bit keys (2048 should be used as min)
  - ECC - Elliptic Curve Cryptography
    - Family of algorithms
    - Does not require as large key sizes
  - DSS - Digital Signature Standard
    - Used for creating digital signatures
    - Enhanced with ECDSA (elliptical curve DSA)
  - ECDH - Diffie-Hellman Key Exchange
    - Used for exchanging symmetric key

Let's Try It Out!

- Open your VM

Exercise - 10 Minutes

- Get in groups of 2 to 3
- Email to the groups your public key
- Have them use your public key to send you a message (keep it appropriate)
- Test if you can decrypt the message using your private key