SECURITY FIRST PRINCIPLES

INFORMATION HIDING - ENCRYPTION

TJ NEL

SECURITY FIRST PRINCIPLES

- Domain Separation
- Process Isolation
- Resource Encapsulation
- Layering
- Modularization
- Least Privilege
- **Information Hiding** 
- Abstraction
- Simplicity of Design
- Minimization

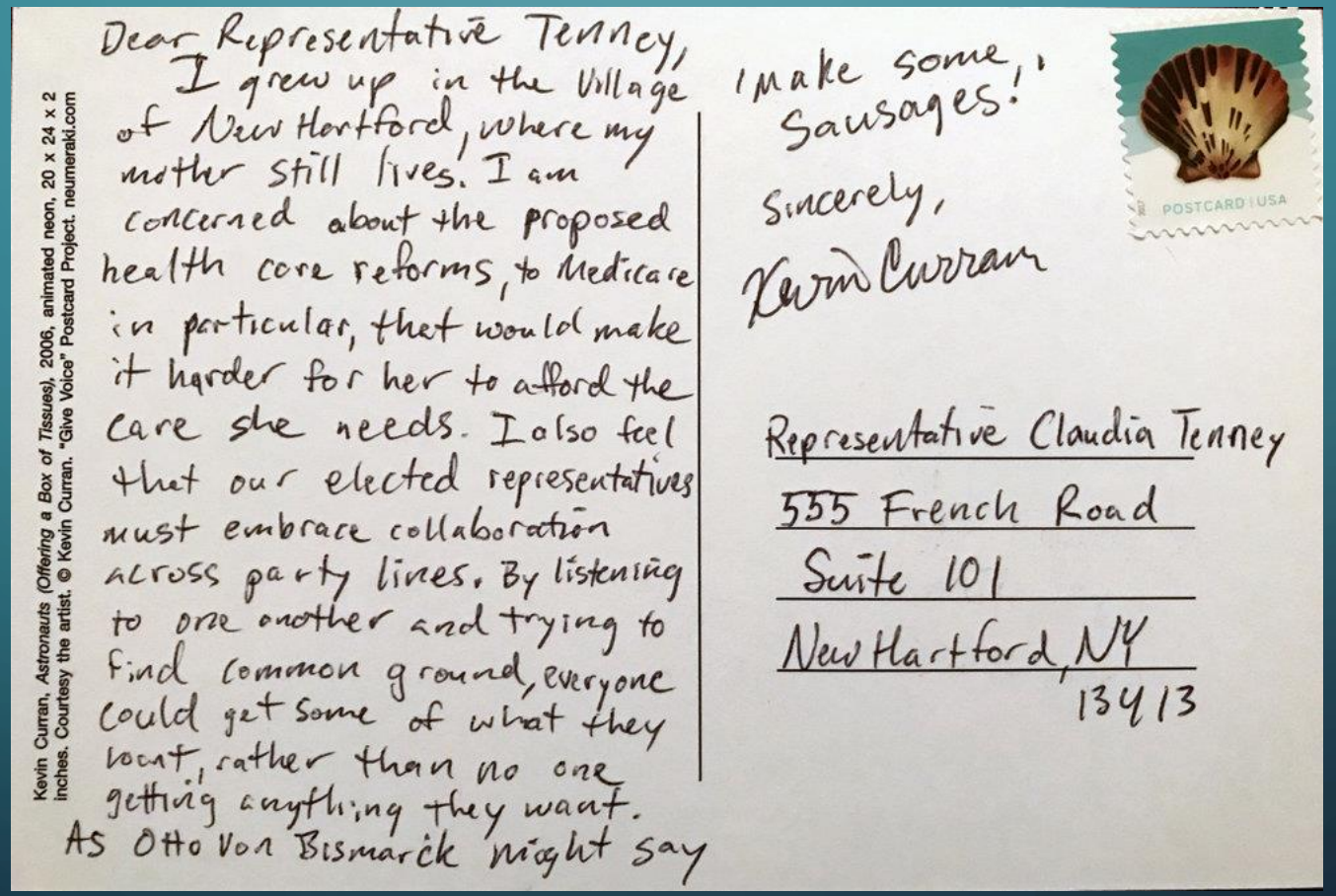
https://users.cs.jmu.edu/tjadenbc/Bootcamp/0-GenCyber-First-Principles.pdf

WHAT IS INFORMATION HIDING?

- Any attempt to prevent people from being able to see information. It can be hiding the content of a letter, or it can be applied to hiding how the letter is delivered. Both ways can prevent people from being able to see the information.

https://gencybercards.com/cards/47

INFORMATION NOT HIDDEN



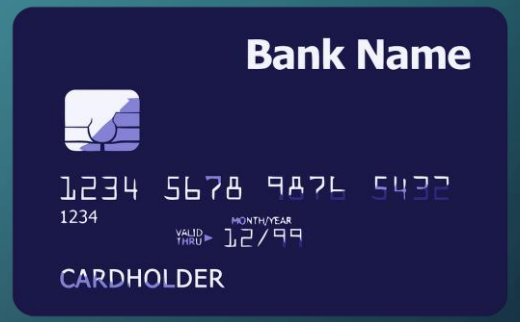
https://neumeraki.com/give-voice/

INFORMATION HIDDEN

https://upload.wikimedia.org/wikipedia/commons/thumb/c/c8/Russia_-_Latvia_1914-11-18_censored_cover.jpg/753px-Russia_-_Latvia_1914-11-18_censored_cover.jpg

WHY WOULD YOU WANT TO HIDE INFORMATION

- Sensitive or personal information can be used by an attacker to
  - Sell for profit
  - Manipulate you into doing something against your will
  - Discredit you or expose unwanted information
  - Gain a strategic advantage against you



ENCRYPTION

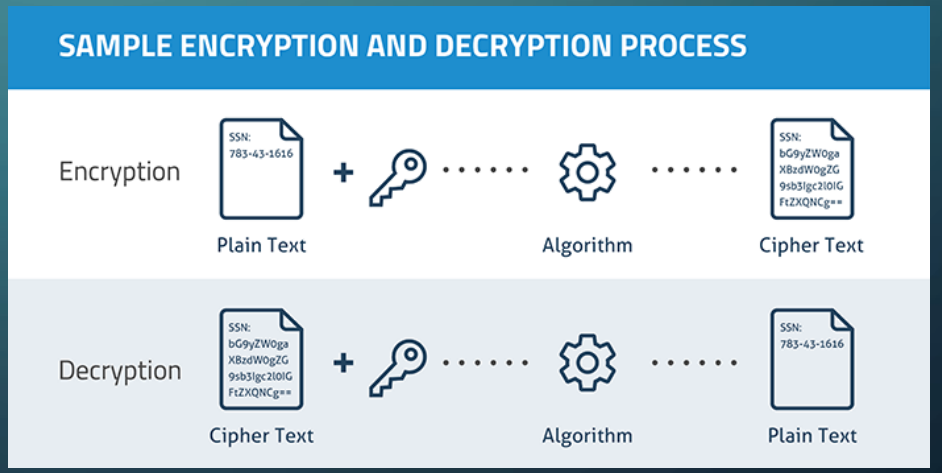
en·cryp·tion

/inˈkripSH(ə)n,enˈkripSH(ə)n/

noun

the process of converting information or data into a code, especially to prevent unauthorized access.

"I use encryption to protect sensitive information transmitted online"



TYPES OF ENCRYPTION

SYMMETRIC

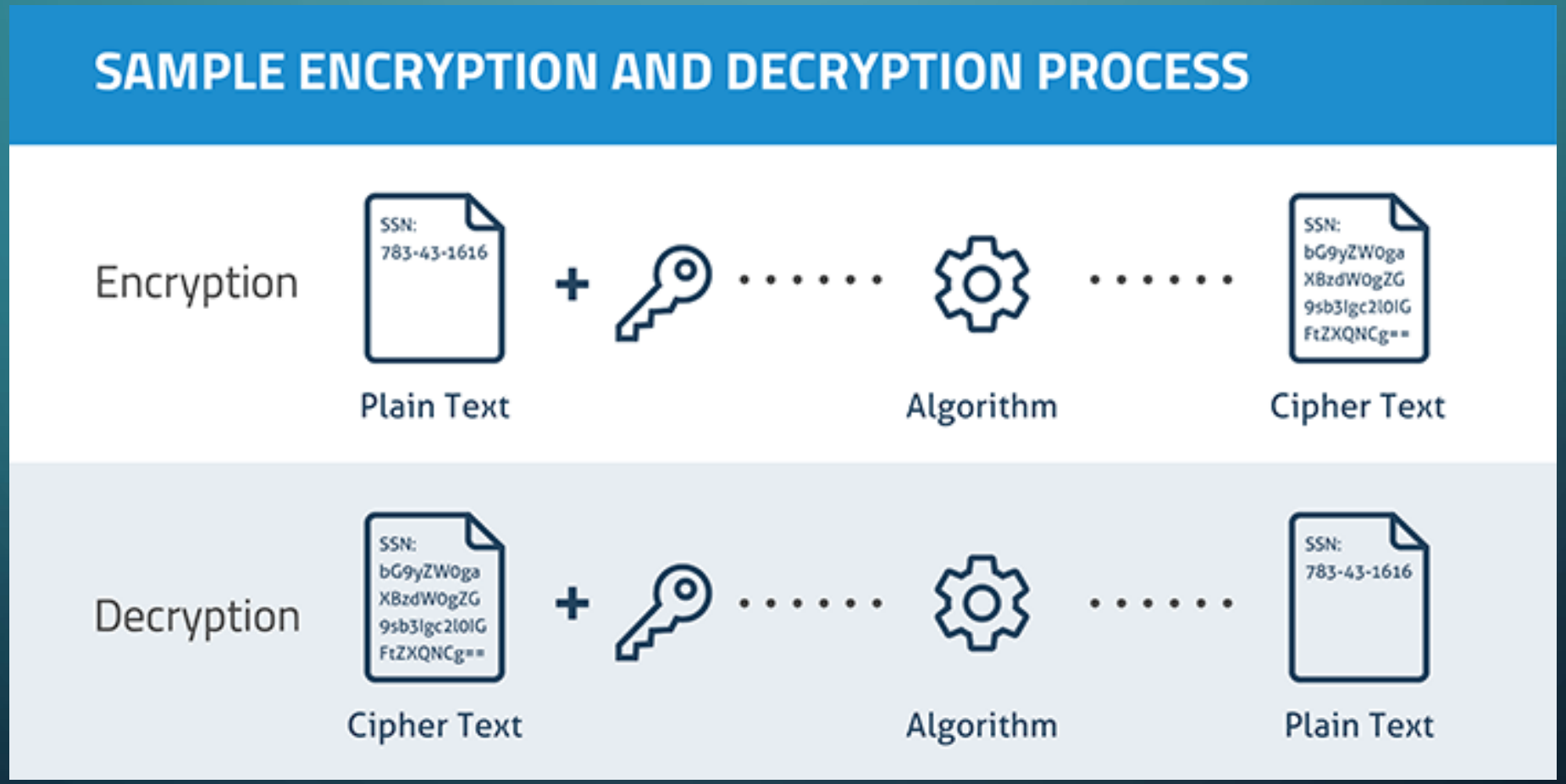
- Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

ASYMMETRIC

- Asymmetric cryptography, is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.

https://en.wikipedia.org/wiki/Public-key_cryptography
https://en.wikipedia.org/wiki/Symmetric-key_algorithm

HOW DOES ENCRYPTION WORK?

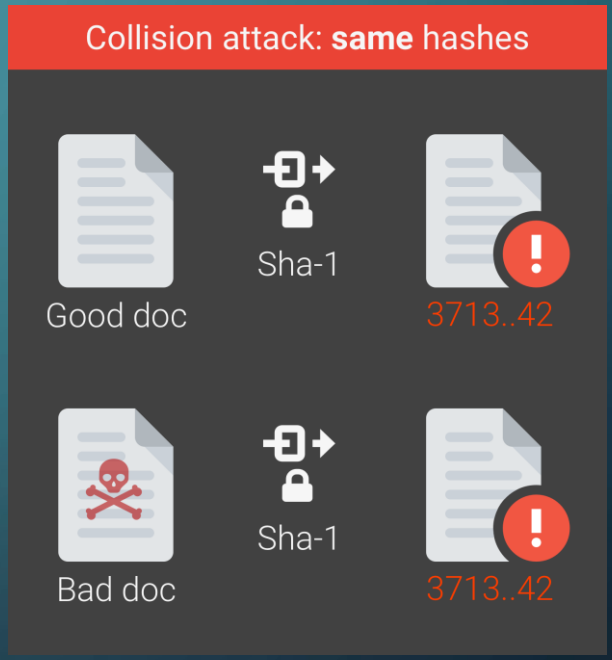


NOT ALL ENCRYPTION IS THE SAME

- There are numerous encryption algorithms and varying degrees of protection.
- All of these algorithms differ in how they work and the keys they use for encryption/decryption tasks.
- Some of these algorithms are so week they can be broken and should not be used
  - Weak Encryption
    - SHA-1
    - RC2
  - Strong Encryption
    - AES
    - SHA-256

SHA-1 GOT… SHATTERED

- SHA-1 Cryptographic Hash Algorithm. A cryptographic hash (sometimes called 'digest') is a kind of 'signature' for a text or a data file. **SHA1** generates an almost-unique 160-bit (20-byte) signature for a text.
- It is now practically possible to craft two colliding PDF files and obtain a SHA-1 digital signature on the first PDF file which can also be abused as a valid signature on the second PDF file.



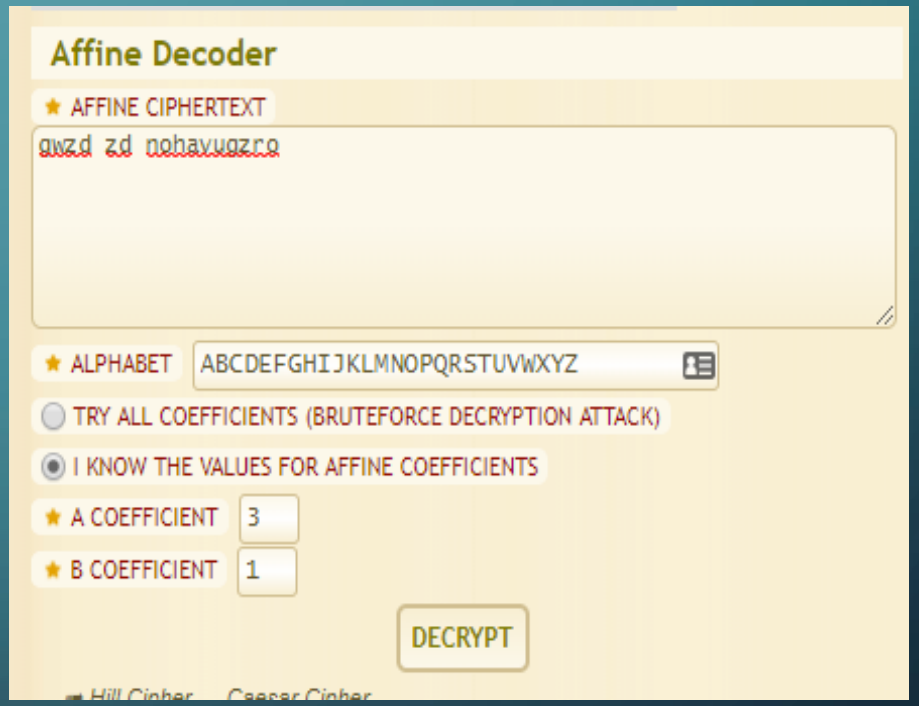
https://shattered.io/

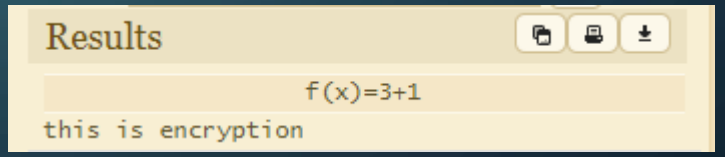
HOW TO USE ENCRYPTION

- Take this encrypted secret message
  - gwzd zd nohavugzro
- We don't know what this represents
  - We could send this to someone else without them knowing our secret
- In order to decrypt, we really need to know:
  - What type of encryption
  - If there are keys needed for this

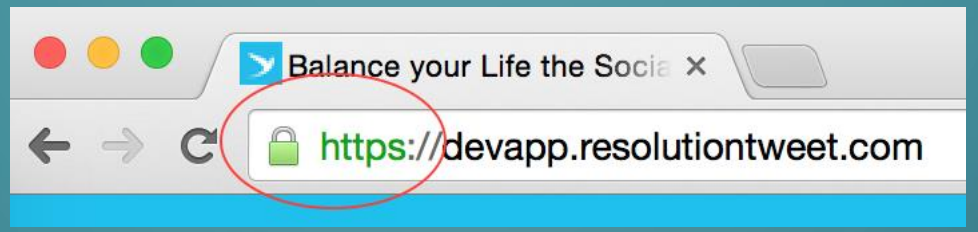
WHEN WE GET THE INFO WE NEED

- Encryption Information
  - Encryption type: Affine Cipher
  - Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - A COEFFICIENT: 3
  - B COEFFICIENT: 1
- When you enter this into the algorithm you get the message
  - this is encryption



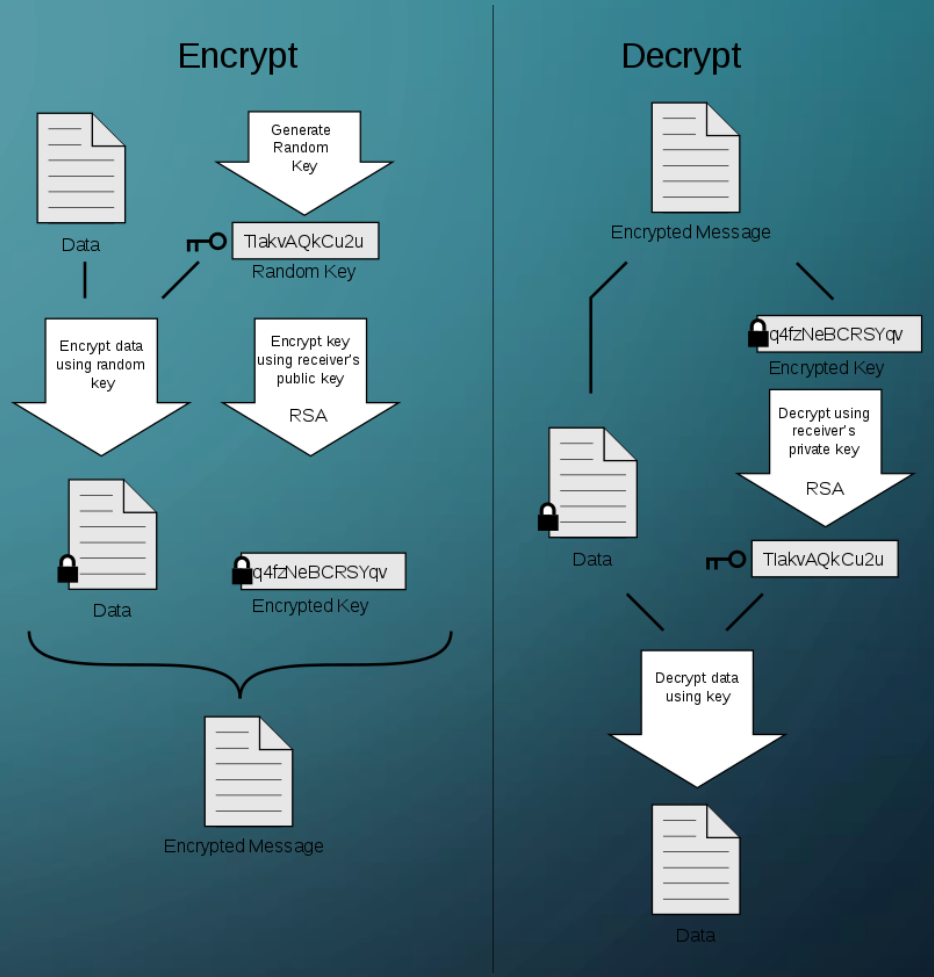


YOU CAN APPLY ENCRYPTION TO REAL WORLD COMMUNICATIONS



PGP PROTECTING EMAIL

- Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.



https://en.wikipedia.org/wiki/Pretty_Good_Privacy

ATTACKING ENCRYPTION

ATTACKERS CAN OBTAIN UNAUTHORIZED ACCESS TO INFORMATION USING SOME KNOWN ATTACK STRATEGIES

- Ciphertext Only Attacks
- Known Plaintext Attack
- Chosen Plaintext Attack
- Dictionary Attack
- Brute Force Attack
- Birthday Attack
- Man in Middle Attack
- Side Channel Attack
- Timing Attacks
- Power Analysis Attacks
- Fault analysis Attacks

THESE CAN BE USED TO GAIN INFORMATION ON THE DATA PROTECTED BY THE ENCRYPTION ALGORITHM

KNOWN PLAINTEXT ATTACK EXAMPLE

- Alice sends a message to Bob encrypted with his public key. Eve overhears an encrypted communication from Bob to Alice, and later observes them meeting at Baker Street . Eve can now guess that the communication contained the word "baker street" somewhere, a form of known plaintext attack.
- Using this information Eve may be able to figure out the encryption and necessary parameters for decryption.
- Affine Cipher is vulnerable to this

https://www.slideshare.net/amiteshg/cryptographyknown-plain-text-attack

- COMPLETE EXERCISES 1-3 AND ASSESSMENT