Encryption at Rest

JJ Quinlivan
Akron Linux Users Group
October 4th, 2018

JJ Quinlivan

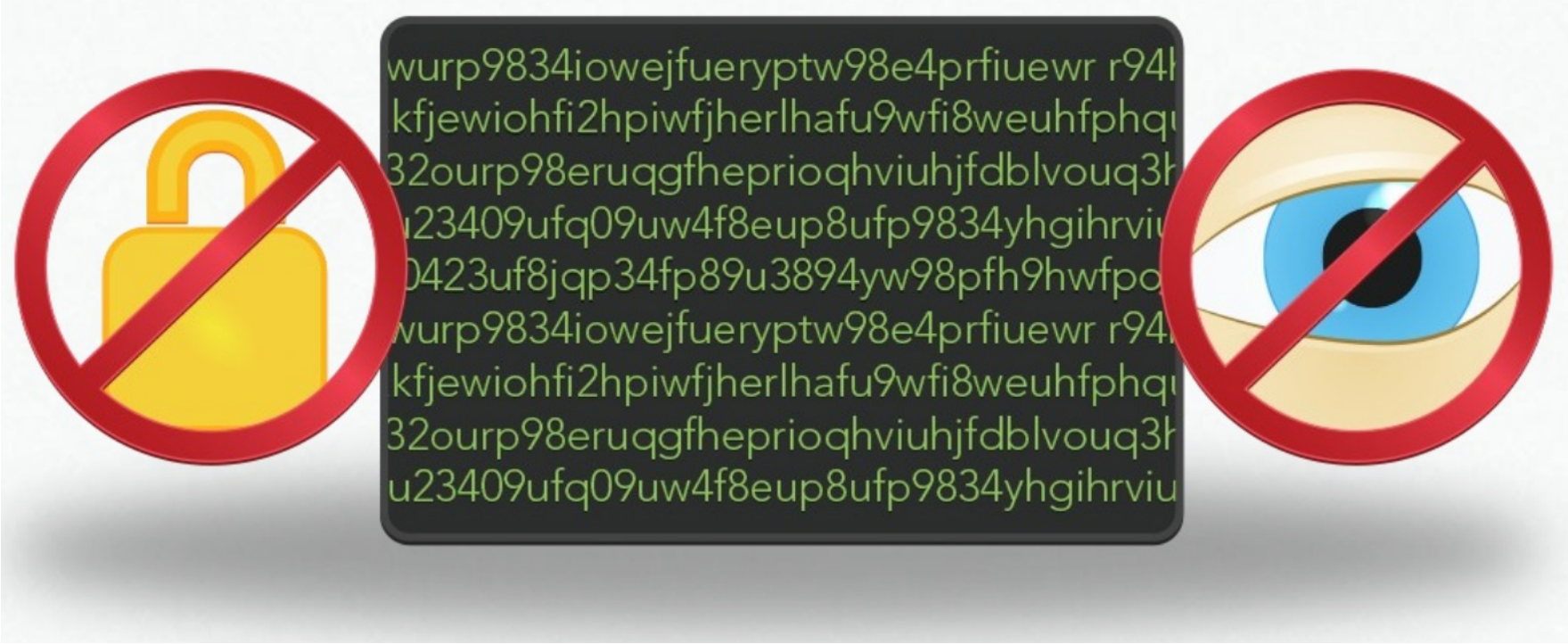
- **Computer Consultant for 25 Years**
- **Disabled for last 10 years**
- **Linux Enthusiast**
  - Lots of time to research and play with Linux and open source software!
- **Not an Expert!**

Agenda

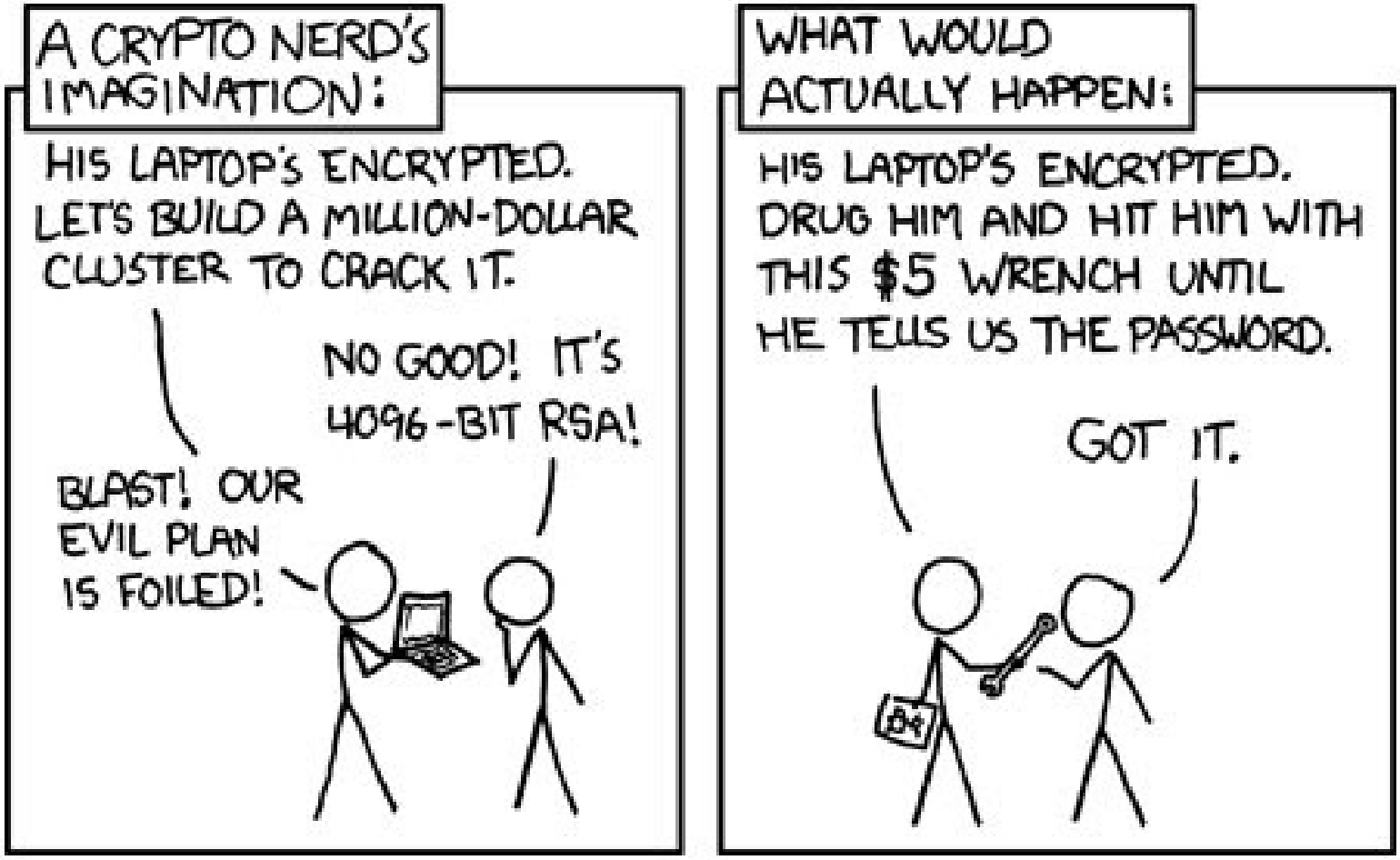
- **Encryption Overview**
- **Encryption at Rest**
  - Full Disk Encryption: SED, LUKS, VeraCrypt
  - File Encryption: Encryptfs, Cryptomator, GPG
  - Encryption in the Cloud: Zero Knowledge

Encryption: What is it for?

- **Encryption is not security**
- **Encryption is about privacy**



Encryption Myths

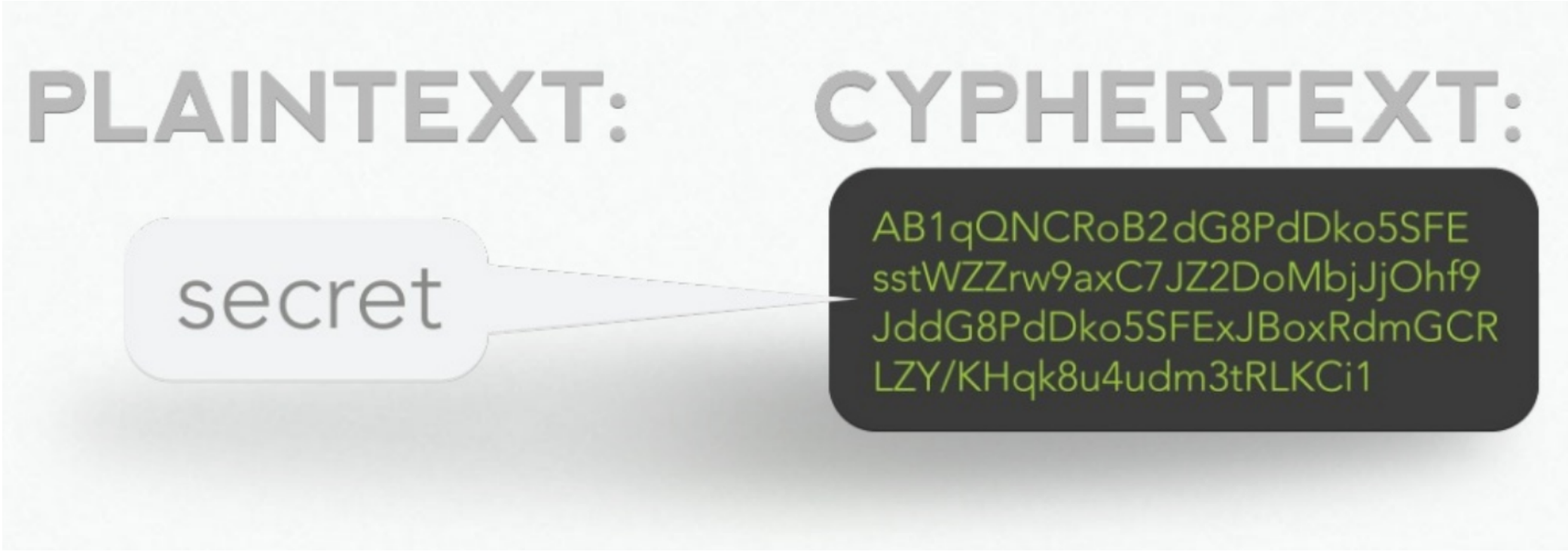


What to worry about

- **Strength of Algorithm used**
- **Prefer Open Source Software**
  - Code can be audited and reviewed by public
- **Hide file structure/location of files**
  - More difficult to locate and decrypt sensitive files
- **Plausible Deniability?**

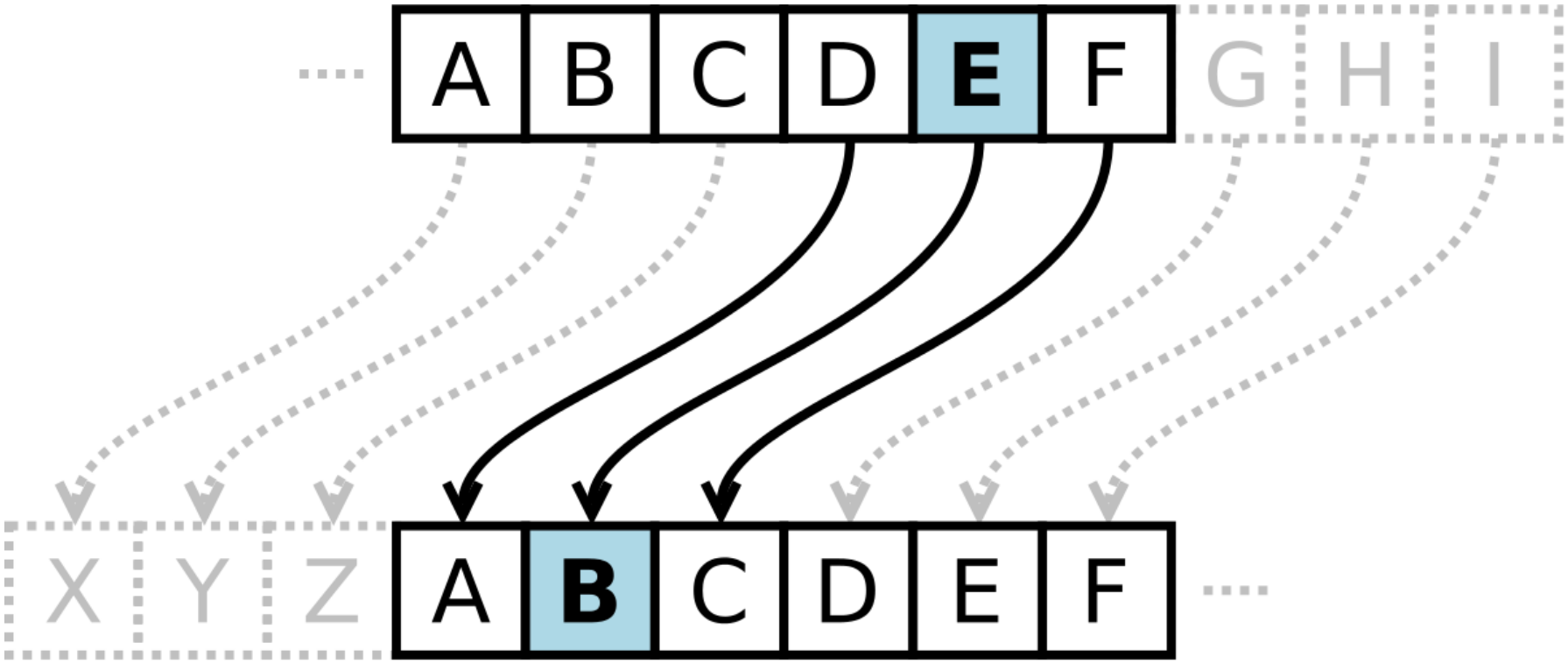
How Encryption Works

- **Uses a encryption algorithm and key to convert data to cyphertext**



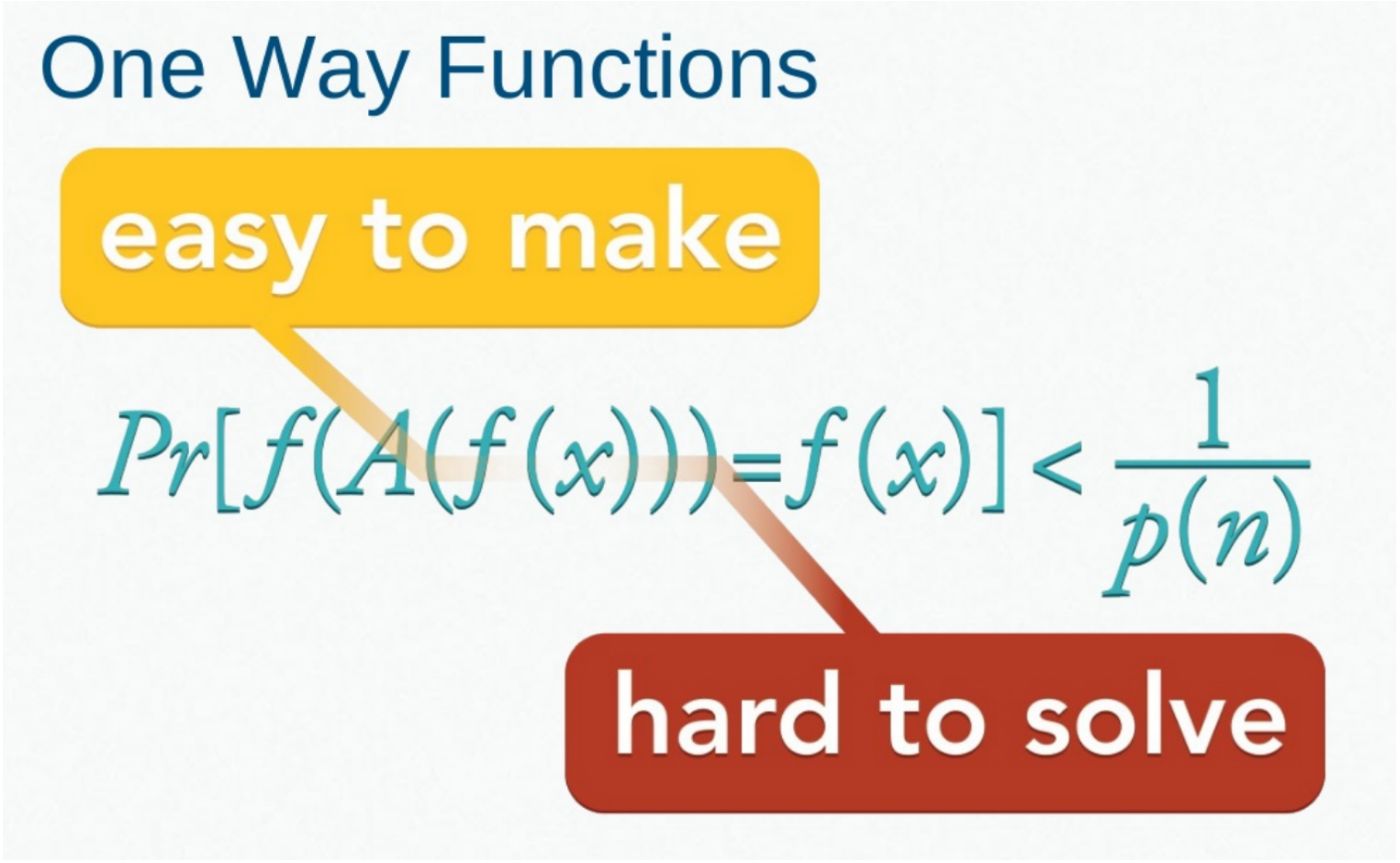
Caesars Cypher

- One of the first recorded encryption standards
- Moved each letter a fixed number of spaces



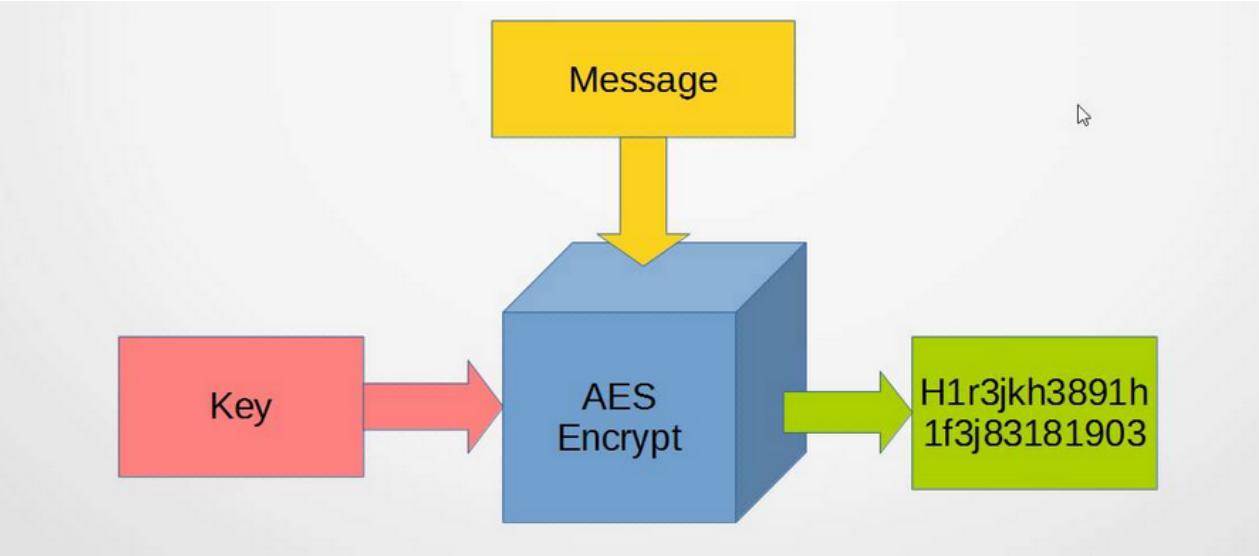
Today's Encryption Algorithms

- **Uses complex math called:**



Advanced Encryption Standard (AES)

- **Adopted in 2001 by NIST**
- **Considered best symmetric algorithm available today**
- **Key sizes of 128, 192, 256 or 512**



Symmetric vs Asymmetric Encryption

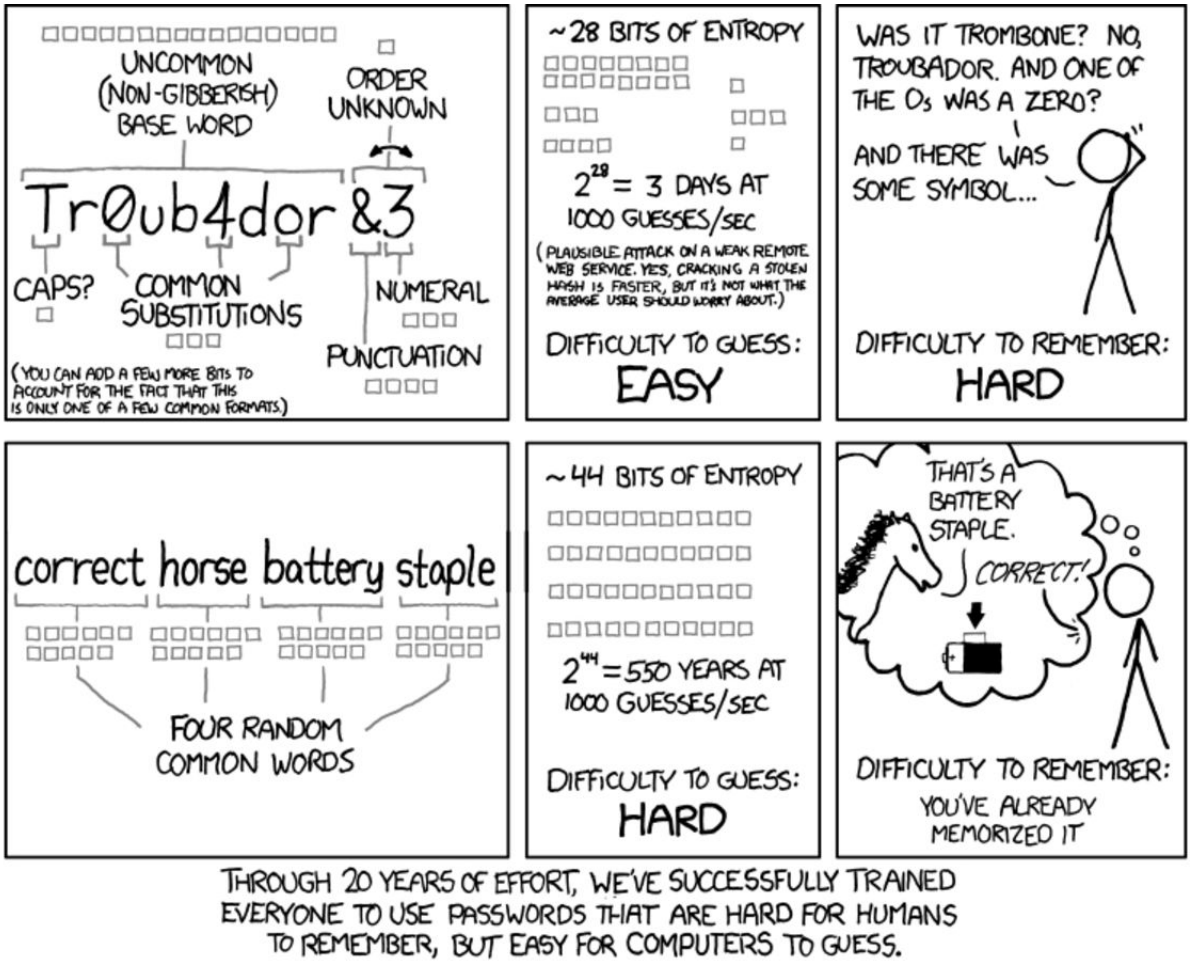
- **Symmetric means the same key used to encrypt the message will also decrypt it**
  - Very efficient = can easily and quickly encrypt and decrypt
  - Key distribution is a problem
- **Asymmetric means uses a key pair one to encrypt, one to decrypt**
  - One of the keys is designated as private, the other public
  - Arbitrary which is which
  - Requires more resources/slower than symmetric

Importance of strong Passphrase

- **Encryption is only as good as the passphrase used to secure it**
- **Use passphrases not passwords**
- **Use Password Manager:**
  - Open Source Password Managers
    - Bitwarden – similar to LastPass
    - KeePassXC – Passwords stored locally
    - Master Password – No stored passwords

Good Passphrases

- **Group of random words**
- **Use Diceware**



Types of Encryption

- **Full Disk Encryption**
  - Protection from Physical Theft, Law Enforcement Seizure
- **File Encryption**
  - Protection of sensitive files while computer is running
  - Protection of files stored in the cloud
- **Encryption in Transit**
  - Not covered today

Full Disk Encryption

- **Self-Encrypting Drives (SED)**
- **DM-Crypt/LUKS**
  - (Linux Unified Key Setup)
- **VeraCrypt**

Use Full Disk Encryption Everywhere

- Don’t Encrypt just your sensitive files
- Anyone who picks up your device even if locked can attach the storage to another machine and access your files
- Your data can be stored in:
- /tmp
- Swapfile
- /var subdirectories

Self-Encrypting Drives (SED)

- **What is it:**
  - Hardware encryption built-in to SSD and spinning disks
  - Opal 2.0 Standard
  - Drives are always encrypted – unlocked until passphrase added
- **How to use it:**
  - Boot drives are split into small hidden boot partition and rest of drive.
  - While locked only small partition is available
  - Download SEDUTIL to lock drives and set passphrase

Self-Encrypting Drives (SED)

- **Pros**
  - Encryption on by default
  - Does not use CPU to decrypt/encrypt
  - Very Fast
  - All drives set with same password
  - Does not require BIOS support (SEDUTIL)
- **Cons**
  - Drive unlocked until PC loses power
  - Drive easily accessible if PC is powered or suspended
  - Does not support External drives
  - Some BIOS confused about boot partitions when locked

Self-Encrypting Drives (SED)

- **When to use:**
  - Desktop Computers
  - Most SSDs support Opal 2.0 standard today

Do not use on Notebooks unless you always poweroff (no suspend)

SEDUTIL

Download SEDUTIL USB Image

```
#linuxpba
DTA LINUX Pre Boot Authorization
Please enter pass-phrase to unlock OPAL drives: *****
Scanning....
Drive /dev/nvme0 Samsung SSD 960 EVO 250GB              is OPAL NOT LOCKED
Drive /dev/sda   Crucial_CT250MX200SSD1                 is OPAL NOT LOCKED
Drive /dev/sdb   Samsung SSD 850 EVO 500GB              is OPAL NOT LOCKED
Drive /dev/sdc   ST500LT025-1DH142                      is OPAL NOT LOCKED
Drive /dev/sdd   Samsung SSD 850 EVO 250GB              is OPAL NOT LOCKED
```

sedutil-cli --initialsetup debug /dev/sdc

sedutil-cli --enablelockingrange 0 debug /dev/sdc

sedutil-cli --setlockingrange 0 lk debug /dev/sdc

sedutil-cli --setmbrdone off debug /dev/sdc

gunzip /usr/sedutil/UEFI64-n.nn.img.gz <-- Replace n.nn with the release number.

sedutil-cli --loadpbaimage debug /usr/sedutil/UEFI64-n.nn.img /dev/sdc <-- Replace n.nn with the release number.

DM-Crypt/LUKS

- **What is it:**
  - LUKS – Linux Unified Key Setup
  - Widely used Encryption standard used in Linux
  - Encrypts Entire drive or partition
  - Can be used to Encrypt Files
  - Many distributions support LUKS encryption for root by default in installer
  - LUKS Header can hold 8 separate passphrases
  - One master key unlocked with passphrase

DM-Crypt/LUKS

- **Pros**
  - Long lasting encryption standard
  - Independently audited
  - Easy to setup
- **Cons**
  - Drive must be wiped to setup
  - *nix only (No Windows/MAC Support)
  - Although rare LUKS header can be corrupted
    - Header can be backed up or even removed

DM-Crypt/LUKS

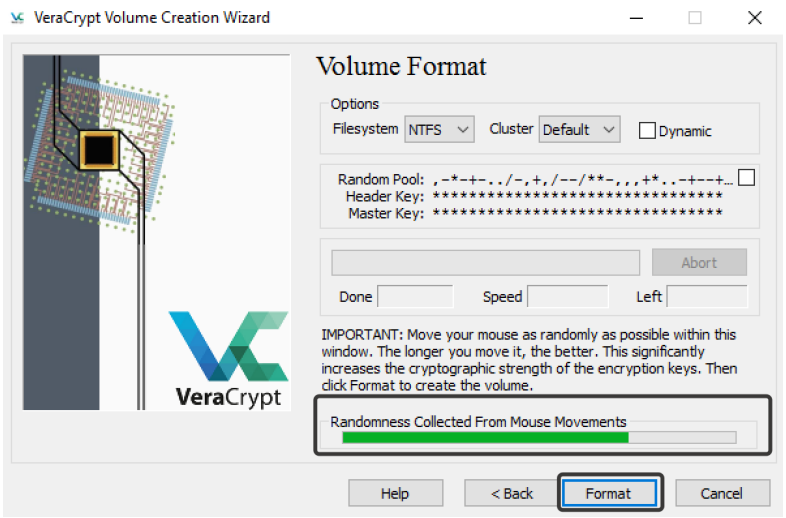
- **When to use:**
  - All bootable drives be encrypted with either SED or LUKS
  - Any USB flash drives that hold sensitive data
  - All drives used for backup

Cryptsetup

Demo

VeraCrypt

- **What is it:**
  - Cross Platform Encryption Software
  - Based on TrueCrypt
    - TrueCrypt no longer updated
    - Fixed security bugs in TrueCrypt
  - Can be used to encrypt drives or files



VeraCrypt

- **Pros**
  - Cross Platform
  - Easy Graphical Interface
  - Can create hidden encrypted partition
- **Cons**
  - More difficult than LUKS to setup as Linux boot/root drive
  - One large container created for file encryption
- **When to use**
  - Need to access partitions between different operating systems

File Encryption

- **Encryptfs**
- **Cryptomator**
- **GPG**

Encryptfs

- **What is it**
  - GPG as a file system
  - Uses master key to encrypt each file in directory automatically
- **Pros**
  - Many distributions make it easy to encrypt home directory with Encryptfs
- **Cons**
  - Linux Only
  - Does not hide filenames
- **When to use**
  - Don’t

Cryptomator

- **What is it**
  - Cross Platform
  - Encrypts files automatically stored in directory
  - Splits files into small encrypted parts
- **Pros**
  - Easy to use
  - Can be used to sync encrypted files between PC and cloud storage (i.e. Dropbox)
- **When to use**
  - Encrypt sensitive files while computer is running or synced to cloud storage

Cryptomator Setup

Demo

GnuPG (GPG)

- **What is it**
  - Open source version of Pretty Good Privacy
  - Both Symmetric and Asymmetric Encryption
  - Primarily used to transfer files/emails to others
- **Pros**
  - Can easily encrypt single file
  - Public/Private Key Encryption and signing
- **Cons**
  - Can be confusing to learn
  - Command line interface
- **When to use**
  - Encrypting an individual file
  - Create for encrypting compressed files (tar files)
  - Sending a file to another person

Encrypt/Decrypt Files with GPG

- **Encrypt Command:**

```
gpg --symmetric --cipher-algo AES256 ~/Documents/PrivateFiles/MyPrivateFile.txt
```

- **Will be asked for a passprase twice**
- **Creates file with .gpg extension**
- **Decrypt Command**

```
gpg -o ~/Documents/PrivateFiles/DecryptedFile.txt -d ~/Documents/PrivateFiles/MyPrivateFile.txt.gpg
```

Other options:

- **Gnome Encfs Manager**
  - Encfs Insecure
- **KDE Vault**
  - Supports Encfs and CryFS
- **KGpg**
- **OpenSSL**

Encryption in the Cloud

- **Zero Knowledge**
  - End-to-End Encryption
  - Cloud storage service has know nothing about your data stored on their servers
  - Data is encrypted and decrypted on the client
  - Service has no access to the encryption key
- **Why?**
  - Service cannot access your data
  - Government cannot demand your data from the cloud service

Encryption in the Cloud

- **Options**
  - Manually with Cryptomator, GPG, etc.
- **Services that provide Zero Knowledge Cloud Storage (for Linux)**
  - tresorit $10.42/200GB
  - pCloud $3.99/500GB + $4.99 for Crypto addon
  - SpiderOak $4.92/150GB
  - iDrive $4.34/2TB (Backup service)