## Encryption and Secure Communications

Ethan Wen

**What is Cryptography?**

Cryptography is the process of converting information/data so that only the intended recipients can access it.

Encryption: transforms plain text into cipher/garbled text through an encryption key

Decryption: transforms cipher/garbled text back into plain text through a decryption key

Cryptography has been used for a long time. Caesar’s cipher - using a cipher to encode/decode information (war plans/actions) so that the enemy would be unable to understand it if the message was stolen or lost in transit. A simple way of securing data since a lot of people were illiterate at that time.

I LOVE CYBER → M PSZI GCFIV

Modern Cryptography: use computationally complex algorithms and keys - A key ~ large binary number.

**Symmetric vs. Asymmetric Encryption:**

Symmetric Encryption/Shared Secret Encryption/Private Key Encryption:

Key used by both parties to encrypt and decrypt messages. Alice and Bob. Both sender and receiver have the same key. The key and the encryption algorithm are applied to transform the plain text into ciphertext (transforming the message into an indiscernible message). Delivered to the recipient either through a secure/insecure channel. The recipient decrypts the message with the reverse of the encryption algorithm and the decryption key (same key) and gets the plain text.

Some algorithms: Data Encryption Standard, Triple DES - using 3 different keys/variations, Advanced Encryption Standards - de facto standard.

Pros and Cons of the Symmetric Encryption:

Faster than asymmetric encryption (1000-10,000), Efficient in computations and storage of data, simplistic yet strong.

If a symmetric key is compromised, then the message is also compromised. Distributing keys is a challenge for large groups (not scalable) needing one key for every person you want to communicate with. No non-repudiation - meaning that you can’t prove who sent it/origination.

Asymmetric Encryptions/Public Key Encryption:

Each user has a public and private key. Public key is available for all users to see while private key is hidden. If one key is used to encrypt, the other is used to decrypt. Alice and Bob example where she encrypts the message with Bob’s Public Key and he decrypts it with his private key. Bob can reply by encrypting his message with Alice’s Public key and she decrypts it with her private key. Because of this setup, repudiation is allowed - where a message can be verified to be sent by said sender → Bob encrypts a message digest (created by mathematical function/hashing function which is one-way function) and then Alice decrypts the message digest and compares the message attached to it after decrypting the text and then running it through a hashing function.

Some algorithms: RSA, Elliptic Curve Cryptography, Diffie-Hellman (mainly used for key exchange). RSA most used right now.

Pros and Cons of Asymmetric Encryption:

No need for secure Distribution of keys, private keys are secure since u don’t need the same key, increased security, scalability

Slower, inefficient for large amounts of data, complex.

Asymmetric and Symmetric Encryption used together for secure key exchange, authentication, and the ability to send bulk data.

**Why is cryptography important?**

Confidentiality: making sure that data remains private/not accessible to non recipients. Whether data is at rest, when it's in transit, and when in use.

Integrity: a way to check if data was altered - encrypted message digests/digital signatures

Authentication: verifies the identity of users.

Non - repudiation: only through asymmetric encryption - verify message sent from sender and prevents sender from denying that they sent it.

**States of data**

Data at Rest: stored data on hard drives, SSDs, USBs. A file stored on Google Drive and

other cloud storage services.

Data in Transit: transmitted data across a network between two or more systems. Sending an email message to your friend.

Data in Use: data that's stored in active memory/currently accessed - writing the email/writing the file.

How encryption of this data could have applied to data in these states?:

Ex: The Hershey Company - September 3-4, 2023: 2214 employee accounts compromised due to a targeted phishing attack - Protected Health Information (medical information) and credit card numbers were potentially compromised.

Ex: Unsecure Network/Public Wifi - sending credentials to a friend to login into an account - network sniffers such as WireShark could potentially intercept this unencrypted data.

Ex: Memory scraping malware - Target’s breach in 2013 - malware installed on POS. Malware captured customer information when processing a transaction - system’s RAM.

**TLS (Transport Layer Security) vs. end-to-end encryption:**

Example (Sending email through Gmail):

When sending messages, data in transit is encrypted from your device to Google’s servers - encrypted on server side and then encrypted again, the outgoing mail server then determines where to send it based on the recipient (DNS lookup) - returning the Mail Exchanger (MX) records for the recipient’s Yahoo server and then transmits the email message through SMTP connection. When data is at rest when those messages are in those servers, the provider’s servers (yahoo and Google) have the technical ability to access and read those messages since they are usually either stored unencrypted or they can encrypt it themselves.

End-to-end encryption: Secure communication where data is encrypted from one end system to the other end system basically meaning that while it travels the data is encrypted while in transit and also at rest. Service providers/servers can’t see the message.

TLS is easier to implement and manage/E2EE more privacy and complex to implement

**What's HTTPS and how does it work?**

HTTPS - Hypertext Transfer Protocol Secure is the secure version of HTTP - protocol that sends data between a web browser and the website’s server. Data is encrypted between you and the website so that no one can eavesdrop on your network.

For instance, data is sent in plain text on HTTP so sensitive information such as credit card information can theoretically be stolen through packet sniffers like Wireshark. General advice for users is to be cautious about visiting web pages/entering sensitive information onto websites that only use HTTP since they weren’t designed with security in mind. However, it doesn't mean that HTTPS respects your privacy or isn’t malicious.

**What are some examples where you might want to use end-to-end encrypted chat instead of just transport-layer encrypted chat?**

You should use end-to-end encryption if you don’t trust the application or service that you are using, the technical infrastructure (servers), and its policies to protect your data against law enforcement requests. The US government can request data from Google’s servers to see your emails through subpoenas, search warrants. Should use end-to-end encryption for highly private information or just by default.

**What is Full Disk Encryption and how do you enable this?**

Full Disk Encryption is a method that encrypts all of the data on one’s hard drive/storage devices - which prevents someone from accessing that data without a passphrase/secret key. Upholds one’s confidentiality - in the case that it was stolen or lost. Uses symmetric encryption - good at bulk encryption. Usually files are automatically encrypted after being written to the disk. Keeping track of your key - password manager - is important since you won’t be able to access your data if you lose track of your password - can lead to permanent data loss.

How to enable Full Disk Encryption?

TPM, UEFI Secure Boot, and specific hardware requirements.

Windows - Home, Professional, Enterprise, and Business

1. Device Encryption - can turn on and encrypts all files
2. BitLocker

Privacy & Security

Save your recovery key

Other changes (which encryption mode to use, whether to encrypt the entire disk)

Restart your computer

MacOS

1. FileVault - recovery key stored on a local file and or iCloud.

VeraCrypt - Cross Platform

LUKS (Linux Unified Key Setup)

iOS - Default encryption - encrypted when locked

Turning on Advanced Data Protection -iPhones

**Ransomware, what does it mean, how does it typical work, and how do decryption works?**

1. Usually through a phishing email, visiting compromised websites, outdated software or vulnerabilities in old OS
2. Ransom Note displayed demanding a payment

Ransomware - malware that encrypts your files with their own key and then holds them hostage until ransom is paid. Threatening business operations and or legal obligations for the company due to data leaks. For an individual, that might be sensitive information or pictures of the victim. In theory, by paying the ransom usually in cryptocurrency, cybercriminals would allow you to decrypt your data by giving you the private key. No guarantee of users/businesses receiving the key/or may not fully recover the files - sometimes they may even ask for a 2nd ransom.

Ransomware payments in 2023 surpassed the $1 Billion mark (Chainalysis)

Sophos State of Ransomware 2022 report, 46% of organizations who paid the ransom received only 61% of their data back.

To prevent ransomware from occurring, install antivirus, update OS to patch vulnerabilities, avoid suspicious emails (don’t download attachments/links from senders you don’t trust), avoid unfamiliar websites. Backing up data to the cloud or to an external device.

**What apps are considered best practice for encrypted communication (instant messaging, email, and browsing)?**

**Instant Messaging:** There are a lot of current applications that support encrypted communication (FB, Instagram, iMessages) but come with complications such as having to opt in/not by default, both parties needing to sign up for this E2EE service, if iCloud Backup is enabled for either sender or receiver without ADP being enabled -> this data isn’t being encrypted end-to-end, complications with users not opting in or having a group chat.

Some good applications for E2EE would be using either Signal, Telegram, WhatsApp.

Signal Protocol - developed in 2013 for instant messaging and video calls

Signal - open-source, nonprofit owned, multiplatform, growing popularity

WhatsApp - popular, disappearing messages and images - however concerns about Meta being obliged to give up metadata (sender, recipient, frequency, what time) and encrypted backups must be turned on for both sender and receiver.

**Email:** Gmail, Outlook, Yahoo Mail, Apple Mail - using TLS - service providers can access (subpoenas/search warrants) content of emails, government data requests, targeted advertising.

ProtonMail - based in Switzerland using E2EE, open source, independently audited, additional privacy features (self-destructing emails, encrypted contacts, email aliases).

Browser Extensions -

Mailvelope/OpenPGP (standard) - using Pretty Good Privacy protocol - hybrid system using both symmetric and asymmetric key systems.

**Browsing:** Brave/Tor Browser - privacy focused browsers

Block trackers and ads by default, HTTPS everywhere - extension that automatically redirects HTTP requests to HTTPs. Brave is more user friendly and faster sometimes. Tor offers multiple layers of encryption/anonymity (routing through multiple servers - makes IP hard to trace).

**What is VPN? When or how should you use one?**

Virtual Private Network creates an encrypted connection between a VPN provider’s server and the Internet Service Provider. Can be used in daily practice but should always be on if you are using public WiFi to prevent others from eavesdroppers. Using protocols such as OpenVPN, IKEv2/IPSEC, WireGuard, SSTP.

Can allow you to bypass geo-restrictions and to hide your IP address, prevent ISP from viewing your internet traffic.

VPN providers - choose a reputable vpn provider, verifies that they keep no logs.

NordVPN, ProtonVPN

Connect to the VPN service before browsing on Public Wi-Fi.

Chapple, M., & Seidl, D. (2021). *CompTIA Security+ SY0-601 Certification Study Guide.* Sybex.

Electronic Frontier Foundation. (2018, November 24). *What should I know about encryption?* Surveillance Self-Defense. https://ssd.eff.org/module/what-should-i-know-about-encryption

Chainalysis Team. (2024, February 29). *Ransomware hit $1 billion in 2023*. https://www.chainalysis.com/blog/ransomware-2024/

Global Cyber Alliance. (2020, October 6). *Communicate securely - GCA Cybersecurity toolkit: Tools and resources to improve your cyber defenses*. https://gcatoolkit.org/journalists/communicate-securely/?\_tk=secure-your-browsing

<https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838#ID0EBD=Windows_11>

<https://gcatoolkit.org/journalists/communicate-securely/?_tk=secure-your-browsing>

(Chapple & Seidl, 2021)

(Electronic Frontier Foundation, 2018)

(Chainalysis Team, 2024)

(Global Cyber Alliance, 2020)