FORTIFY CYBERSECURITY EDUCATION SERIES

June 04, 2024

CYBER HAWAII

ABOUT CYBERHAWAII

CyberHawaii is an information sharing and analysis non-profit organization committed to developing and enhancing Hawaii's cybersecurity capabilities

- CyberHawaii is committed to a whole community approach that will help to:
  - Mitigate cyber risks for all community members
  - Develop educational and workforce pathways for students
  - Augment cyber services being delivered by government agencies, commercial entities, research organizations and Community Based Organizations
  - Inform local decision makers about cyber security risks and solutions
- Founded 2016
- Part of CyberUSA network
- Supported by corporate memberships and grants

CYBER HAWAII

CURRENT MEMBERS & KEY PARTNERS

GROWTH MEMBERS

Bank of Hawaii
Booz | Allen | Hamilton
DataHouse
First Hawaiian Bank
Hawai'i Pacific Health — Kapi'olani, Pali Momi, Straub, Wilcox — Creating a Healthier Hawai'i
Hawaii State Federal Credit Union — always right by you
Hawaiian Electric, Maui Electric, Hawai'i Electric Light
Hawaiian Telcom — Hawai'i's Technology Leader
Kamehameha Schools 1887 — I Mua
Matson
referentia
UHA Health Insurance
University of Hawai'i System
Zippy's Restaurants

SUSTAINING MEMBERS

Central Pacific Bank — Works. For You.
Hawai'i Gas — The Clean Energy Company
Hawai'i Community Foundation — Amplify the Power of Giving
Delta Dental — HDS — Hawaii Dental Service
hmsa
SERVCO
Techmana
DRFortress

STRATEGIC GOVERNMENT PARTNERS

Department of Justice, Federal Bureau of Investigation
NSA/CSS Hawaii — Kīnā'ole
U.S. Department of Homeland Security
U.S. Pacific Command
State of Hawai'i 1959
Cybersecurity & Infrastructure Security Agency
Office of Homeland Security, State of Hawaii
City and County of Honolulu — State of Hawai'i
Board of Water Supply — City and County of Honolulu

STRATEGIC AFFILIATES

Chamber of Commerce Hawaii
Hawaii Business Roundtable Incorporated
HIEDB — Hawaii Island Economic Development Board
CIO Council of Hawai'i
Hawai'i Visitors & Convention Bureau
ISSA — Information Systems Security Association — Hawai'i Chapter
mauieconomic development board
Transform Hawai'i Government

CYBER HAWAII

CYBER HAWAII

Fortify Cybersecurity Webinar Series

Sponsored with support from the
Department of Business, Economic Development & Tourism

CYBER HAWAII

Fortify Cybersecurity Webinar Series

Sponsored with support from the
Department of Business, Economic Development & Tourism

Encryption

ADMINISTRATIVE

- Enter questions into chat box
- The presenter has agreed that you can contact him after the presentation if you have questions or would like more information
- Please remain on mute during the presentation until designated Q&A sessions

CYBER HAWAII

PRESENTER

J.R. Lilo

CISA Region 9 first Cybersecurity Law Enforcement Liaison

FAAIUASO.LILO@cisa.dhs.gov

CISA
CYBER+INFRASTRUCTURE

CYBER HAWAII

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Faaiuaso Lilo (JR)
Cybersecurity Advisor - Law Enforcement Liaison
(Los Angeles, California)

ENCRYPTION

Faaiuaso Lilo (JR)
June 04, 2024

Who is CISA?

From CISA's Website: [About CISA | CISA]

- CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.
    - One of the entities that falls under the Department of Homeland Security.
    - We are designed for collaboration and partnership. Learn about our layered mission to reduce risk to the nation's cyber and physical infrastructure.
    - Work with partners to defend against today's threats

What is Encryption?

Definition of Encryption:

- A method where information is converted into secret code that hides information's true meaning.

Why is it important?

- Securing various types of IT assets and more importantly, personable identifiable information (PII).
- Works with four essential functions:
  - Confidentiality
  - Authentication
  - Integrity
  - Nonrepudiation

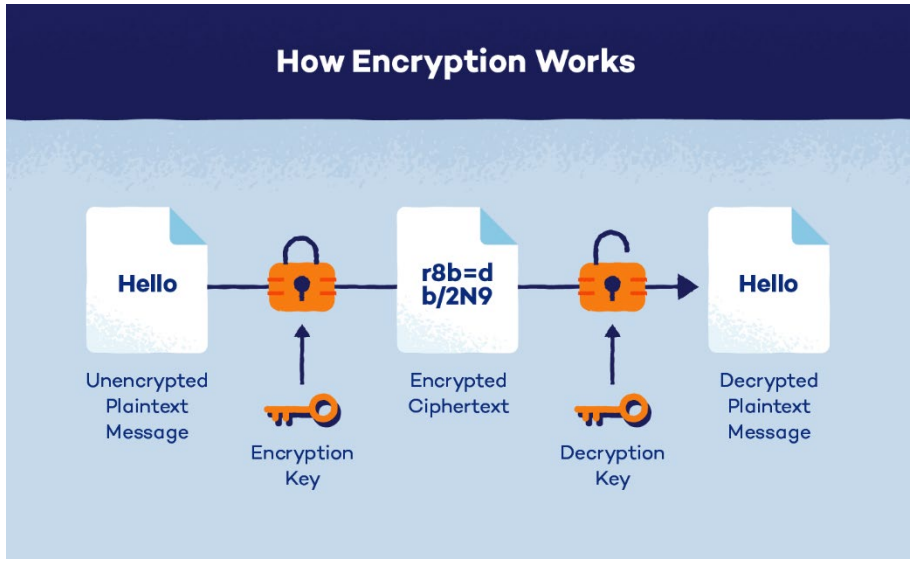
Sources: What is Encryption and How Does it Work? | Definition from TechTarget, What is encryption? How it works + types of encryption – Norton

How Does Encryption Work?

How does encryption work?:

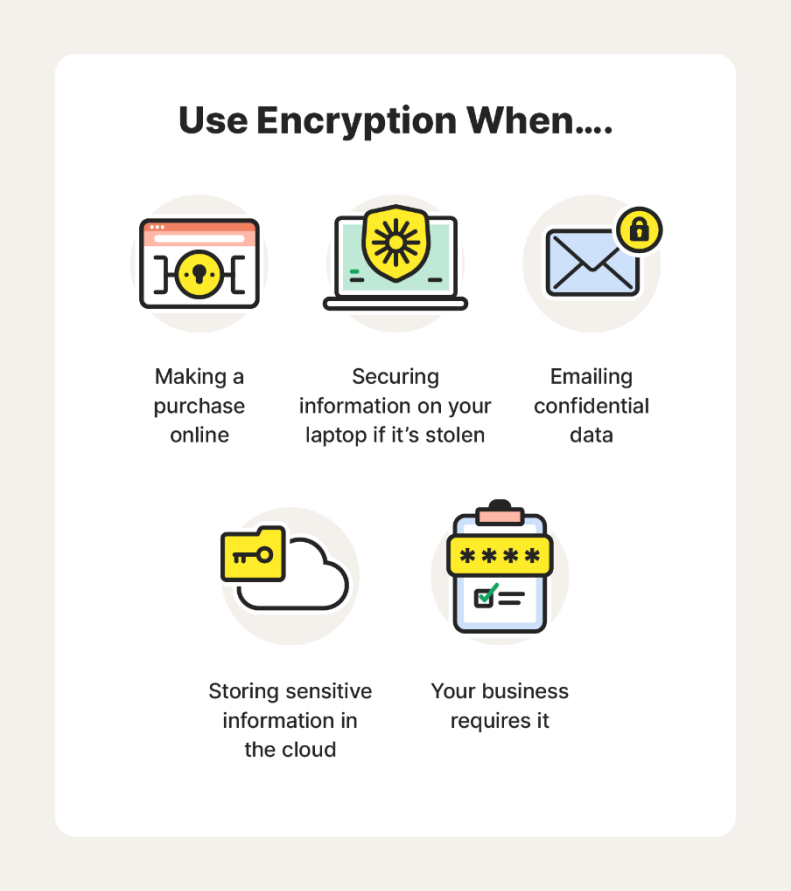
- It is a mathematical equation; involves cryptography keys.

- Other factors include;
  - Encryption Algorithms
  - Ciphertext
  - Plaintext



When to Use Encryption:

When do you use encryption?:



Source: [What is encryption? How it works + types of encryption – Norton]

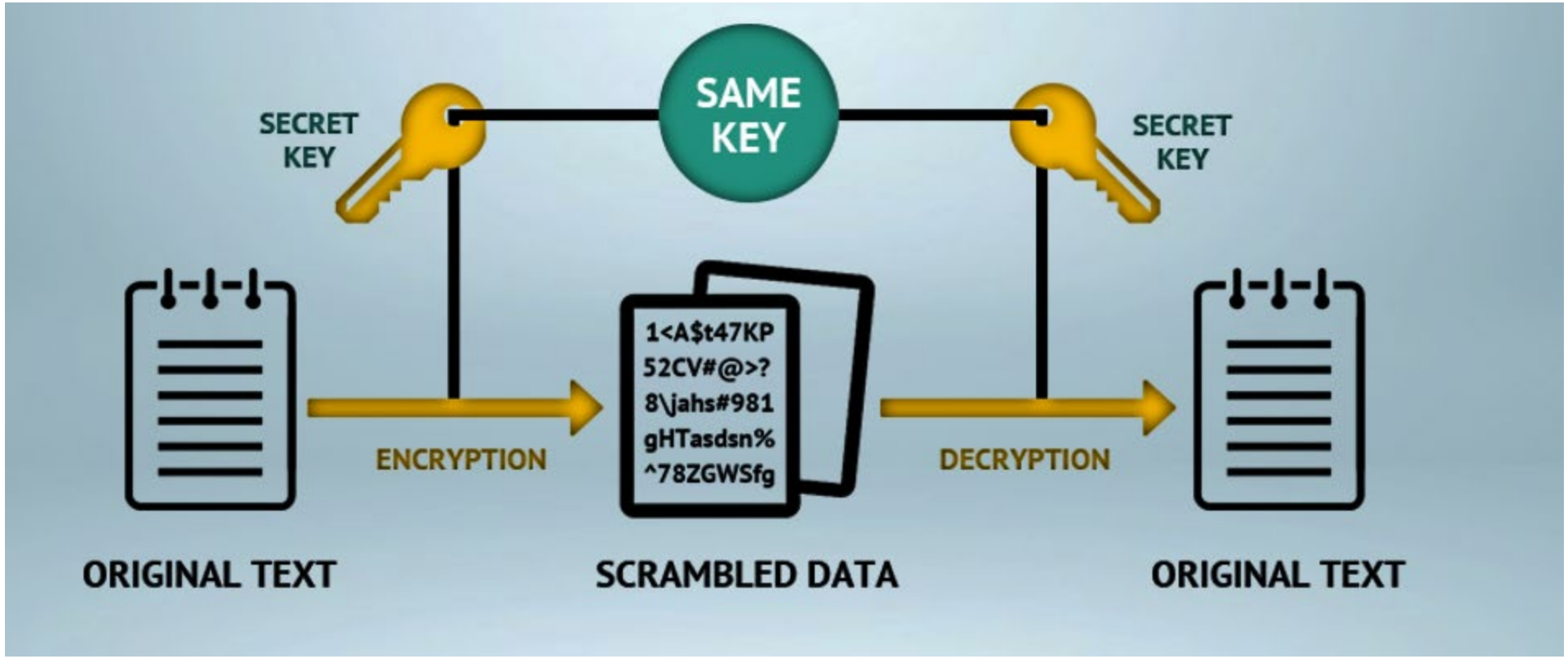
Symmetric Key Cryptography:

- **Symmetric**:
  - Private key cryptography, secret key cryptography, or single-key encryption.
  - Utilizes one key for both the encryption process and decryption process.
  - Each user must have access to the same private key
    - These private keys are shared from an established secure comms channel
    - Secure key exchange method: Diffie-Hellman key agreement.
  - Two types of Symmetric Key Algorithms:
    1. **Block Cipher**: Works on a fixed-size block of data.
       - Block size is 8; 8 bytes of plaintext are encrypted at a time.
    2. **Stream Cipher**: Convert one bit (or byte) of data at a time.
       - Generates a keystream based on the provided key. Keystream is XORed with the plaintext data.
         - What is XOR? Another way of saying "Exclusive OR operation." If the input has at least a 1 value, then it has a 1 XOR output. But if both inputs has the same value, then it has a 0 output value.
         - Truth Table:

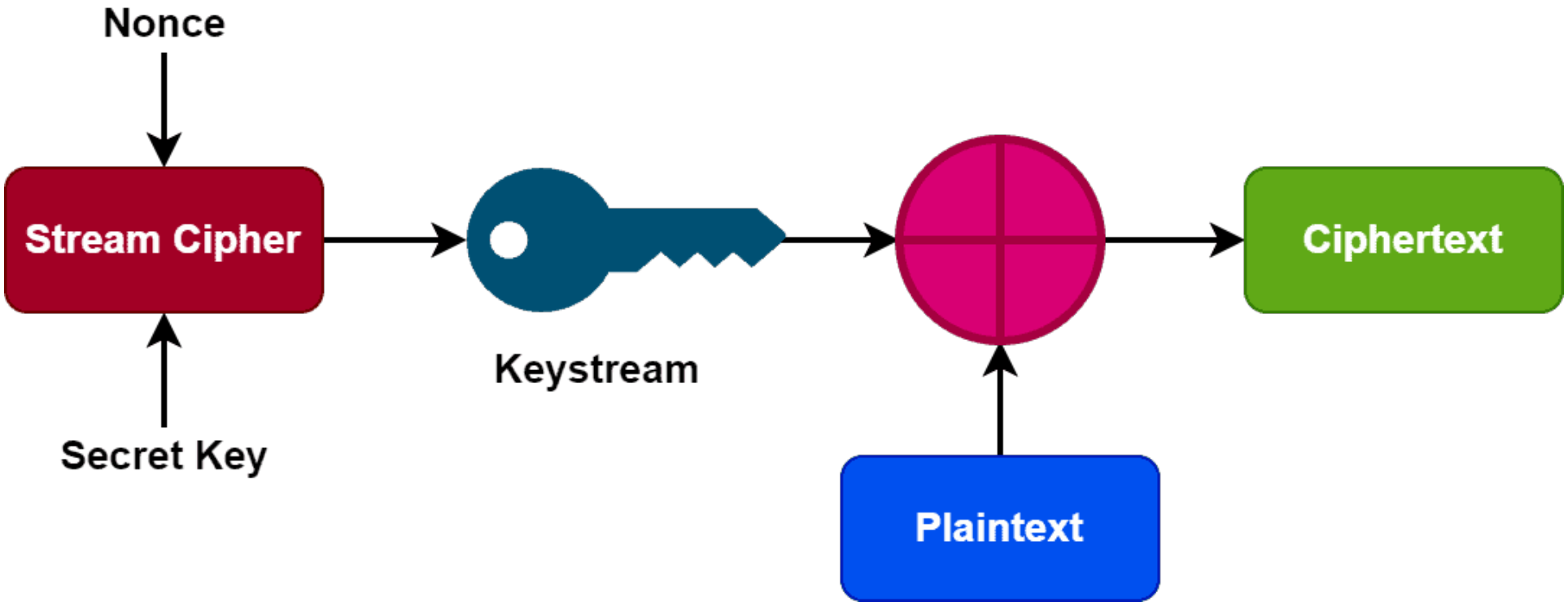
A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

Sources: Types of Cryptography | IBM and Logical XOR (Glossary Entry) – Embedded Systems (plymouth.ac.uk)

Symmetric Key Process:



Stream Cipher Process:



Symmetric Key Advantages:

Key Advantages:

- **Security**: Secure and normally requires users to keep track of one key.
  - Highly secure when it uses a secure algorithm.

- **Speed**: Symmetric encryption only requires one key, which makes it simple and less resource-intrusive.

- **Smaller size**: Symmetric key ciphers smaller in size; quick when encrypting and decrypting data.

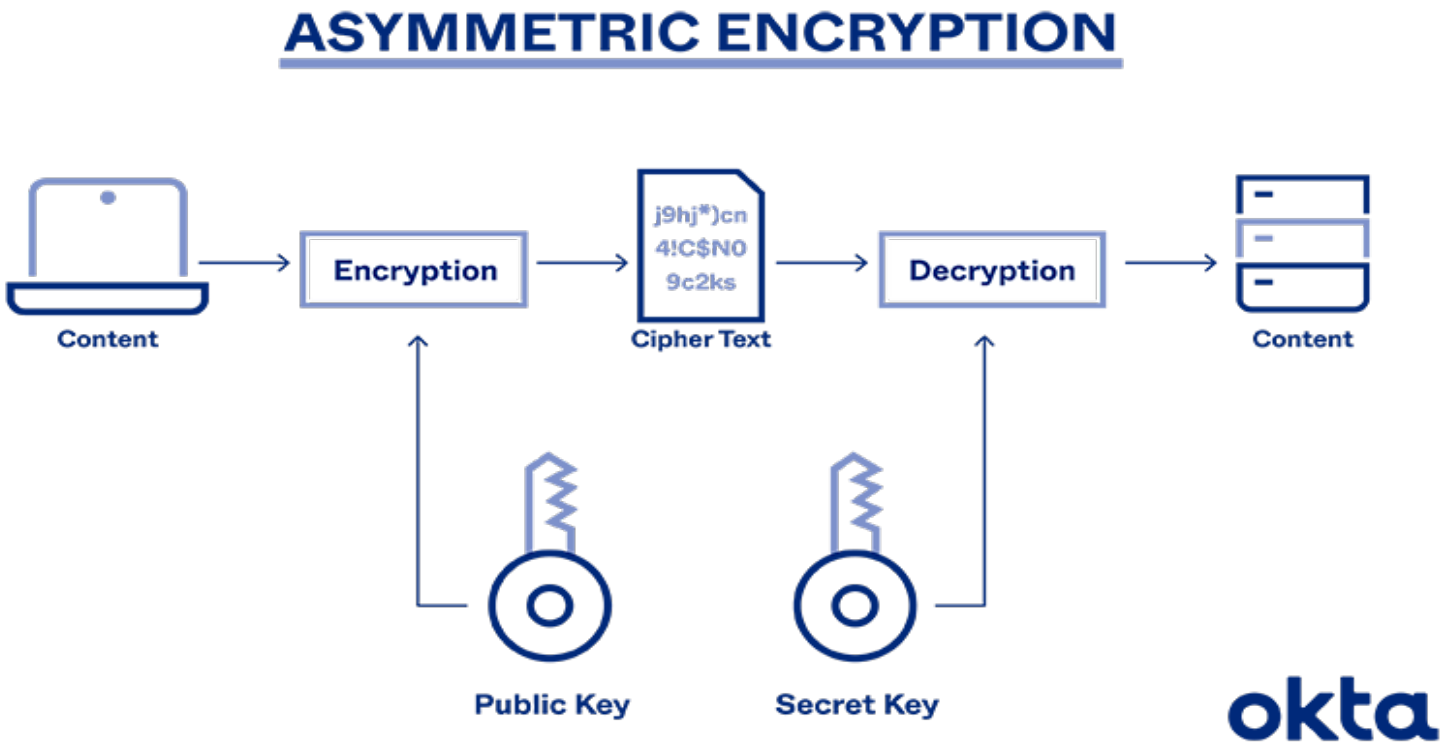
- **Efficient in handling large volumes of data**.

Asymmetric Key Cryptography:

- **Asymmetric**:
  - Public-Key cryptography, utilizes a pair of keys to encrypt and decrypt data.
  - Two keys:
    1. Public key: shared with anyone
    2. Private key: kept secret by the owner
  - Asymmetric process:
    - Sender uses recipient's public key to encrypt the data, then the recipient uses their private key to decrypt the data.

Source: What is Asymmetric Encryption? - GeeksforGeeks

Asymmetric Key Process:



Source: [Asymmetric Encryption: Definition, Architecture, Usage (okta.com)]

Asymmetric Key Advantages:

Enhanced Security:

- Provides a higher level of security compared to symmetric encryption. Utilizes two keys, one for encryption and another for decryption. Harder for attackers to decrypt data.

Authentication:

- Receiver can verify sender's identity by using the sender's public key to decrypt their message.

Non-Repudiation:

- Sender cannot deny sending a message or altering contents due to the message being encrypted by the sender's private key and only their public can decrypt it. No tampering.

Key Distribution:

- Eliminates the need for secure key distribution system that is required in symmetric encryption.

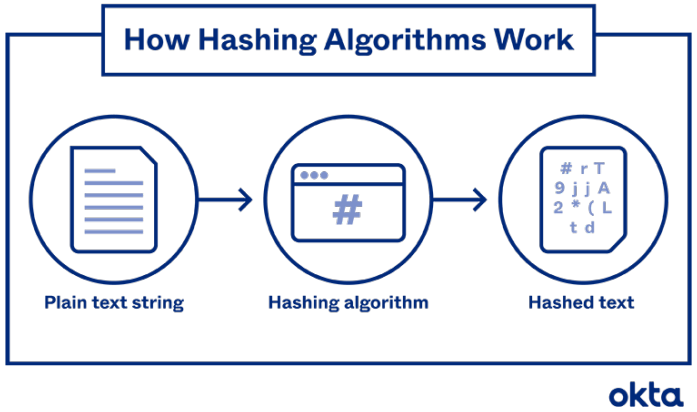
Versatility:

- Used for wide range of applications such as secure email communication, online banking transactions and e-commerce for secure SSL/TSL connections, used for secure internet traffic.

Hashing Algorithms:

What is the Hashing Algorithm?

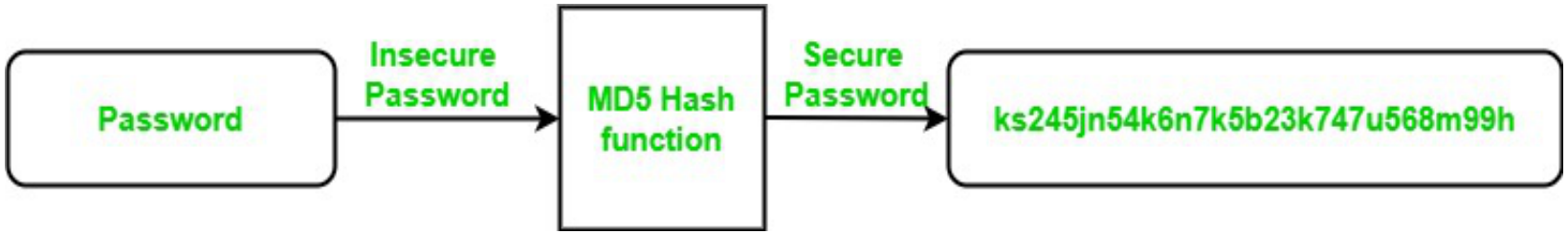
- A hashing algorithm is a mathematical function that garbles data and makes it unreadable.
  - One-way programs, so the text can't be unscrambled and decoded by anyone else.
  - Hashing protects data at rest.



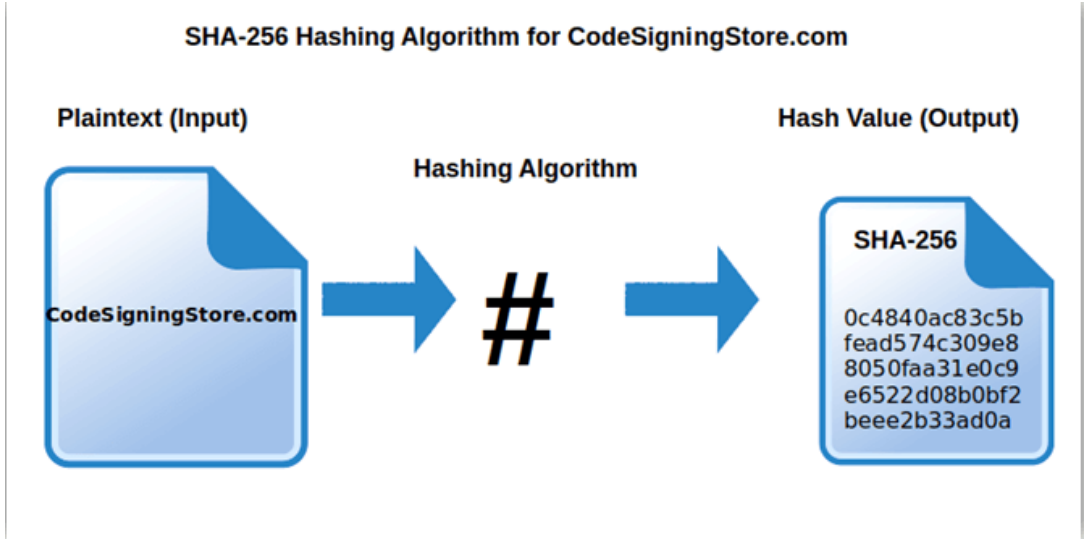
Hashing Algorithms:

Common Hashing Algorithms:

- MD-5 Hash:
  - Example: 72b003ba1a806c3f94026568ad5c5933



- SHA-256: f6bf870a2a5bb6d26ddbeda8e903f3867f729785a36f89bfae896776777d50a

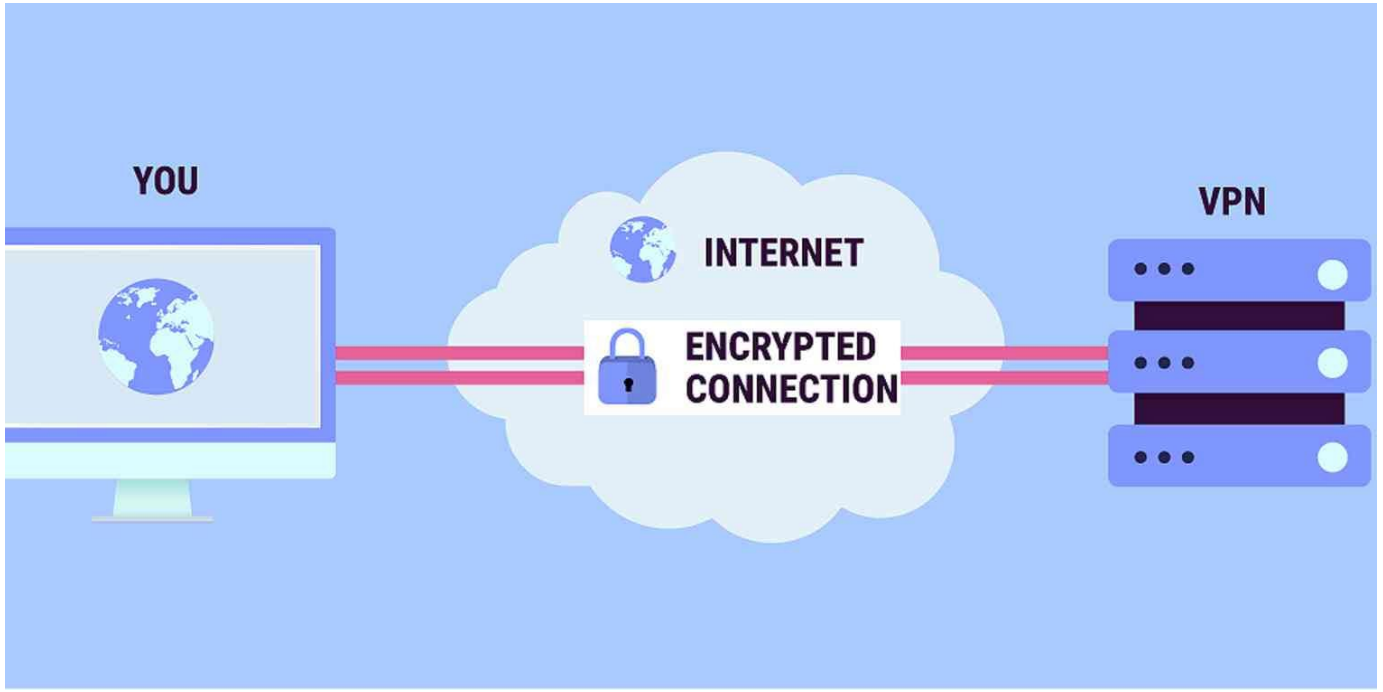


VPN Services:

What is a Virtual Private Network?

- Encrypted connection over the Internet from a device to a network

How does it work?



VPN Advantages:

Why do Businesses use VPN Services?

- Provide remote employees access to internal network.
- Prevent web traffic from being exposed on the open Internet.
- Provide end-to-end encryption for every device in the company's network.
- Secure remote access to a remote network over the internet

DNS Encryption:

What is DNS? DNS is the abbreviation for the “Domain Name System” and is essentially the phonebook system of the internet.

- **DNS over TLS (DoT)**

- **Secure DNS (or DNS over HTTPS)**:
  - Encrypts DNS traffic that flows between a browser and websites visited.
  - Stops attackers from intercepting or altering the data.
  - Performs DNS resolutions via HTTPS
  - Deployed through an app or as a proxy on a nameserver

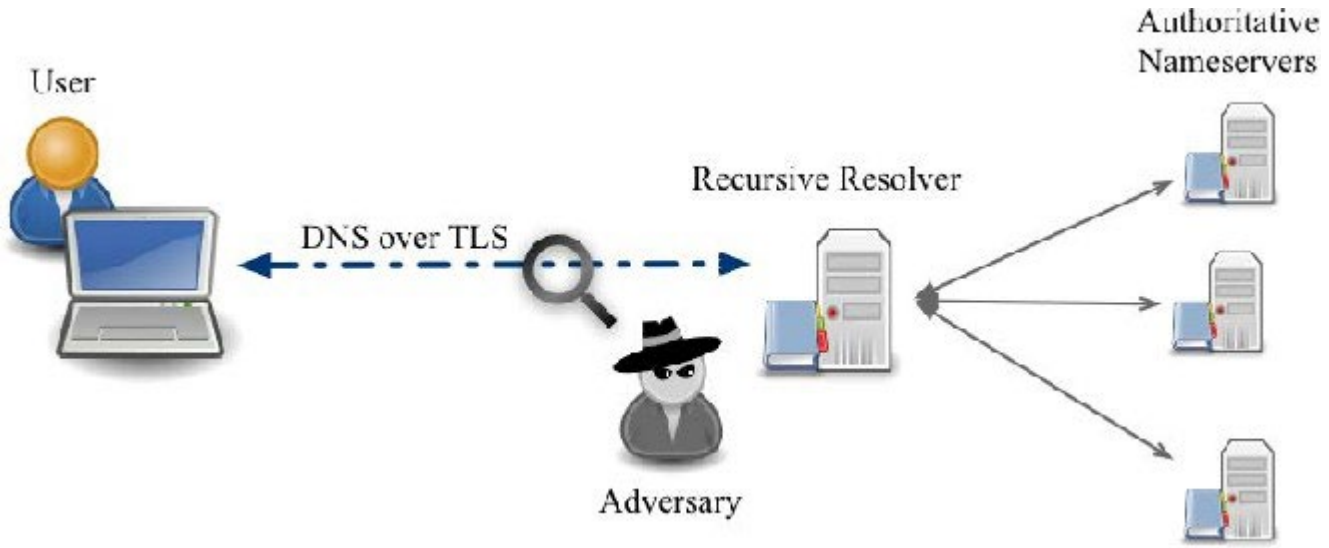
- Unencrypted DNS Risks.

- DNS Encryption Advantages.

DNS Encryption:

- DNS over HTTPS:

- DNS over TLS:

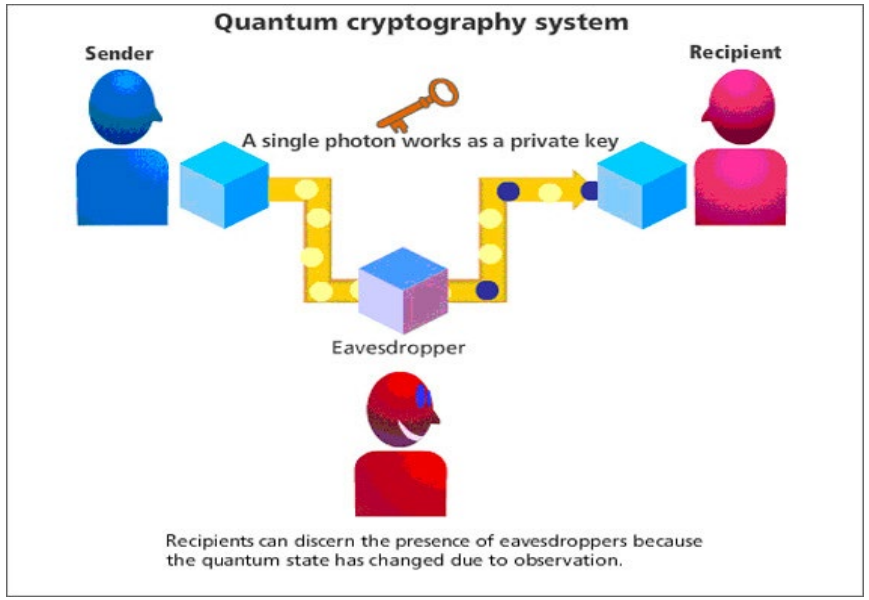


Quantum Cryptography:

Concept: Utilizes the laws of quantum physics to transmit private information.

Quantum Key Distribution (QKD); most widely studied quantum cryptography.

- Uses a series of photons to transmit a secret, random sequence, known as the key.

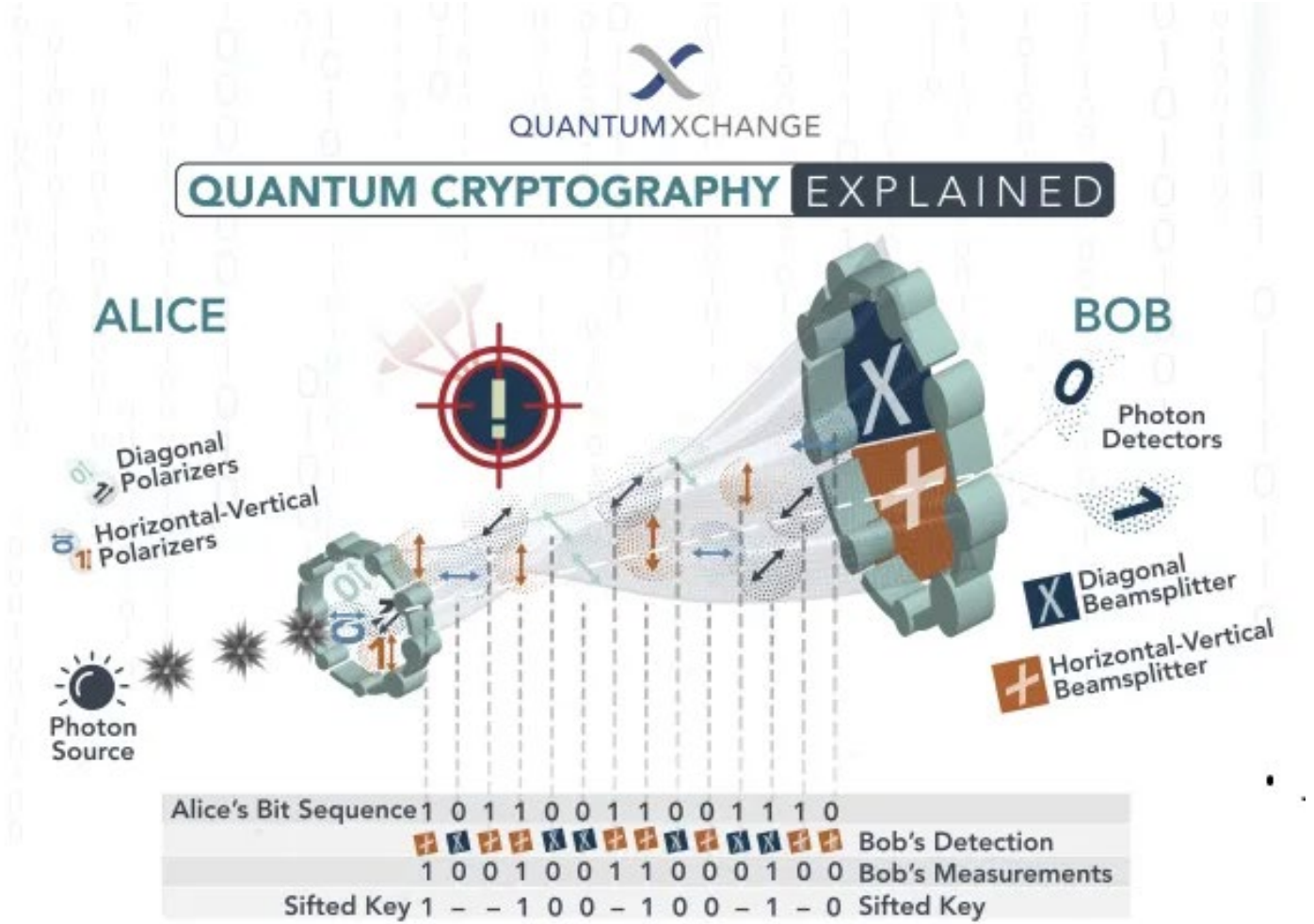


Quantum Key Distribution by IBM: Example

Source: What Is Quantum Cryptography? | IBM

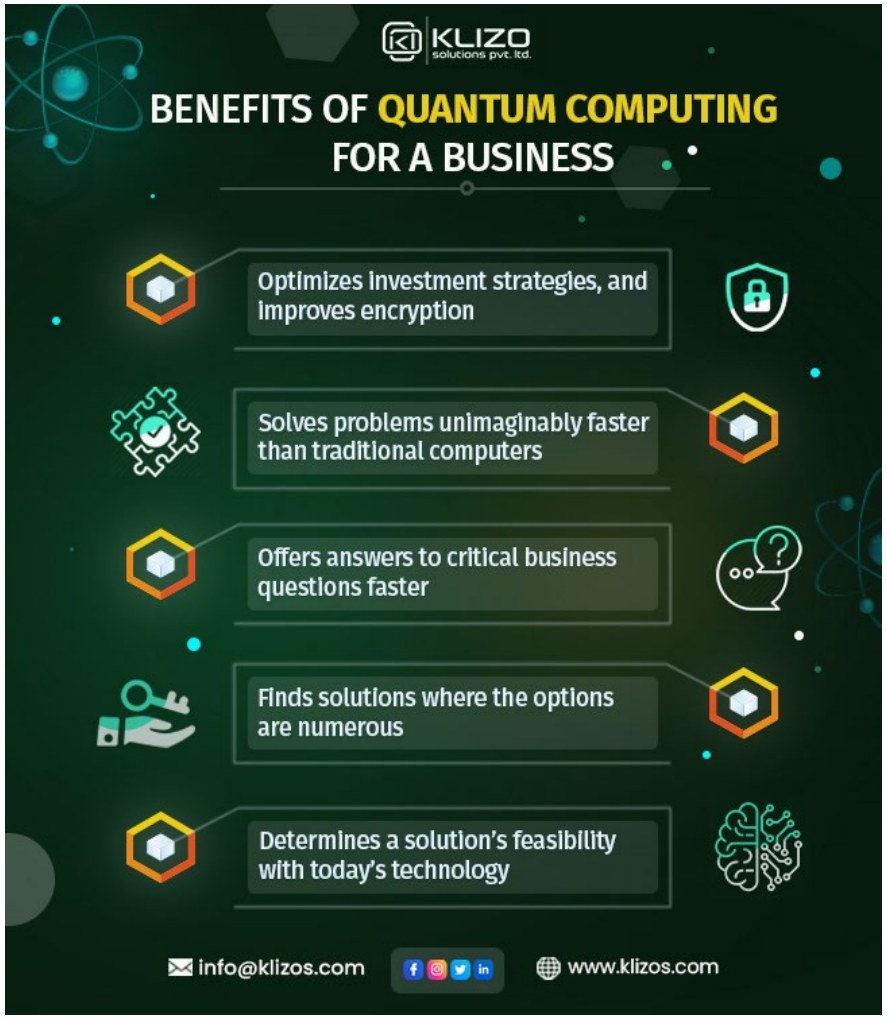
Quantum Cryptography:

Quantum Key Distribution (QKD) Process:



Quantum Computing for Businesses:

Key advantages for Quantum Computing for businesses:



Source: [What Are The Benefits Of Using Quantum Cryptography? - Capa Learning]

Questions?

FAAIUASO L. LILO ("J.R.")
Cybersecurity Advisor / Law Enforcement Liaison (Los Angeles, CA)
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency (CISA)
Region 9 (AZ, CA, NV, HI, AS, CNMI, GU)
Work Cell: 202-702-9233 |
Email: faaiuaso.lilo@cisa.dhs.gov

NEXT STEPS

Contact information

- **J.R. Lilo**
  - CISA Region 9 first Cybersecurity Law Enforcement Liaison
  - FAAIUASO.LILO@cisa.dhs.gov

Next in the Fortify Cybersecurity Series

- Mobile Device Management & Remote Access; or Secure by Design
  - Tuesday July 09, 2024
  - Registration will be on CyberHawaii.org website
- More Information
  - Al Ogata, al.ogata@cyberhawaii.org

CISA CYBER+INFRASTRUCTURE

Mahalo

CYBER HAWAII