Introduction to Cybersecurity

Elvira Popeea

Bogdan Dan

Agenda

- About SecureWorks
- Basic concepts & Definitions
- Cybersecurity in E.U. & Romania
- Security Roles
- Fundamental Principles of Security
- Q&A

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

Threat

Any potential danger that is associated with the exploitation of a vulnerability

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Information Security Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies

Risk

The likelihood of a threat source exploiting a vulnerability and the corresponding business impact.

Malware

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system

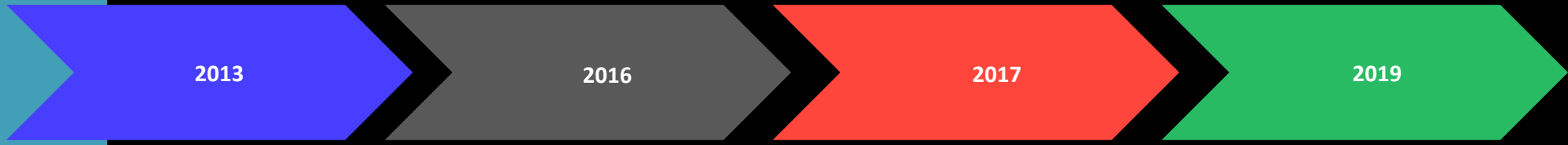
Security Patch

Software or operating-system patch that is intended to correct a vulnerability to hacking or viral infection

Control (Countermeasure)

Measures put in place to mitigate (reduce) the potential risk

Cybersecurity in Europe



- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

- European Commission adopted a Communication on strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry;
- The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU

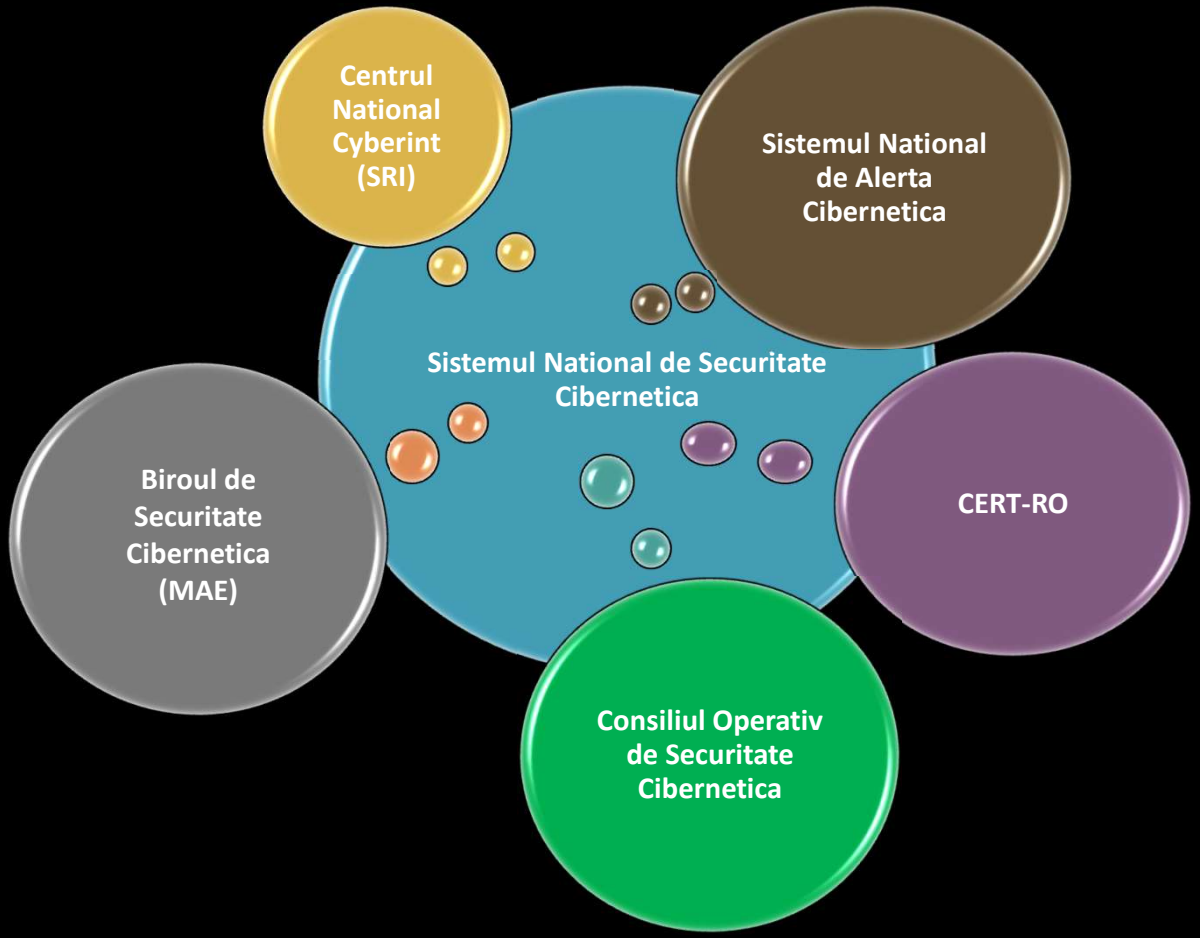
- Resilience, Deterrence and Defense: Building strong cybersecurity for the EU
- Framework for a Joint EU Diplomatic Response to Malicious Cyber Activity

- Cyber Diplomacy Toolbox a framework for a joint EU diplomatic response: UE can impose travel restrictions, assets freeze for participants in cyberattacks

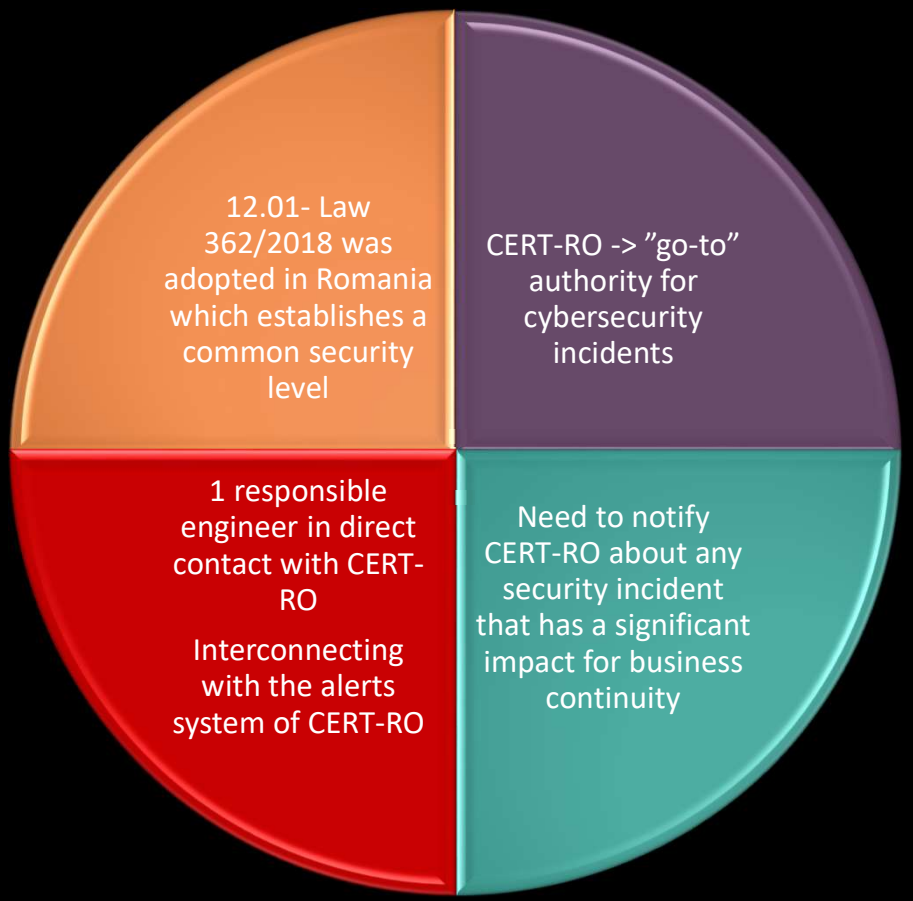
European Union Agency for Network and Information Security

- Recommendations on cybersecurity and independent advice
- Activities that support policy making and implementation
- ‘Hands On’ work, where ENISA collaborates directly with operational teams throughout the EU
- Bringing together EU Communities and coordinating the response to large scale cross-border cybersecurity incidents
- Drawing up cybersecurity certification schemes, the development and evaluation of National Cybersecurity Strategies
- Drawing up cybersecurity certification schemes, the development and evaluation of National Cybersecurity Strategies
- CSIRTs(Computer Security Incident Response Team) cooperation and capacity building

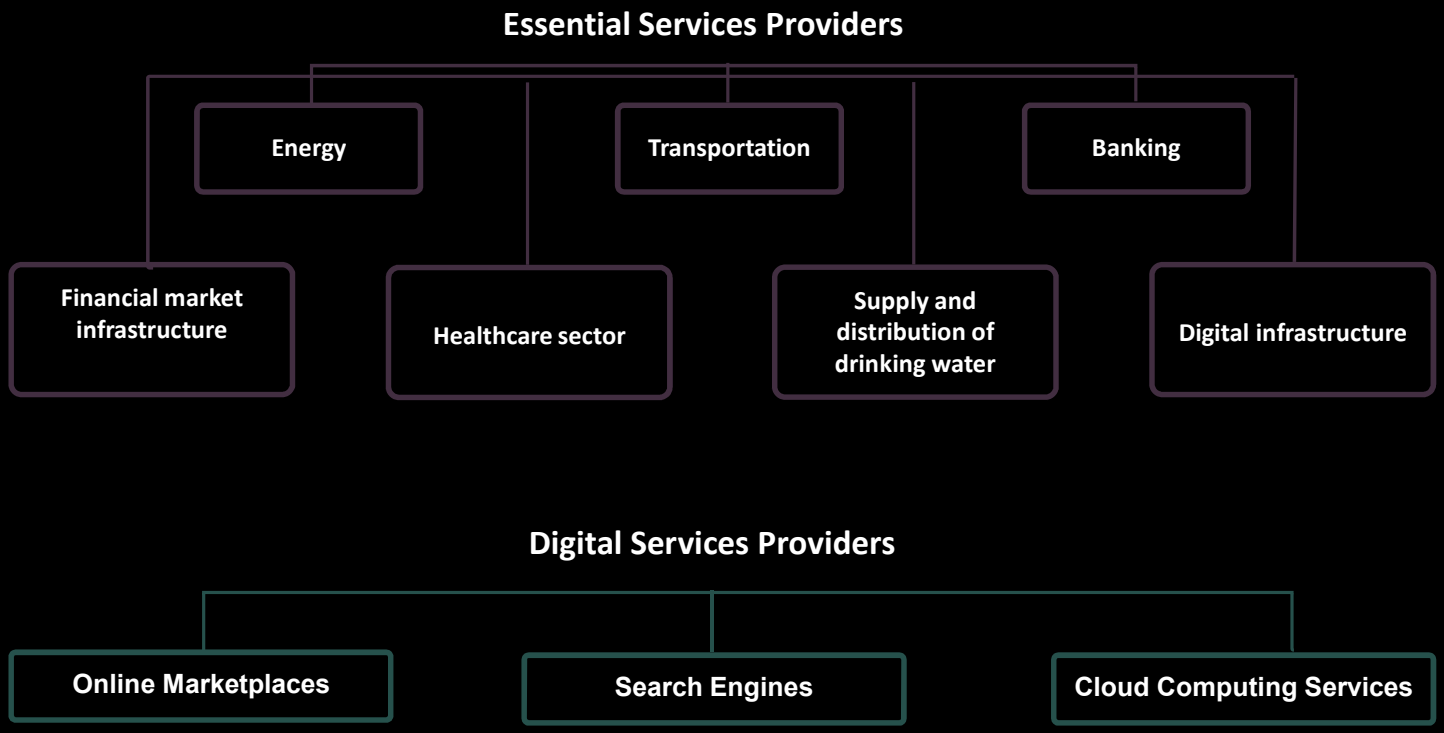
Romanian National Structures with roles in Cybersecurity



Law 362/2018


12.01- Law 362/2018 was adopted in Romania which establishes a common security level
CERT-RO -> ”go-to” authority for cybersecurity incidents
1 responsible engineer in direct contact with CERT-RO
Interconnecting with the alerts system of CERT-RO
Need to notify CERT-RO about any security incident that has a significant impact for business continuity

Law 362/2018


Essential Services Providers
Energy
Transportation
Banking
Financial market infrastructure
Healthcare sector
Supply and distribution of drinking water
Digital infrastructure
Digital Services Providers
Online Marketplaces
Search Engines
Cloud Computing Services

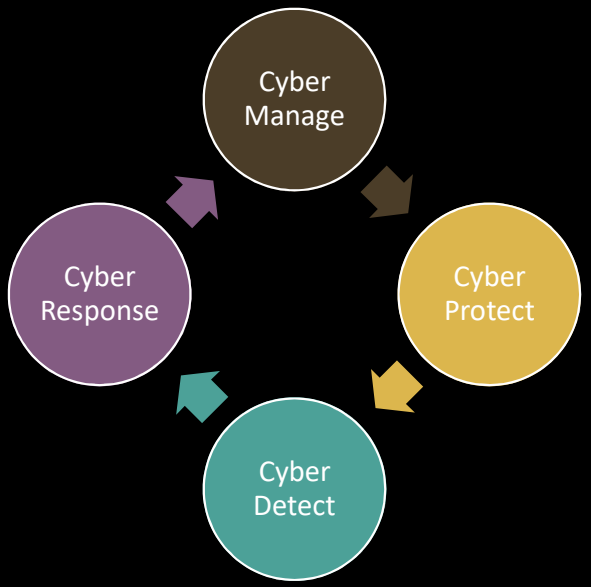
Law 362/2018

1. Cyber Manage- Defining policies and procedures for the company's cybersecurity

2. Cyber Protect – Protection against cyberattacks
Protection of data

3. Cyber Detect – Detection of issues in the system
Reporting security incidents

4. Cyber Response – responding to security incidents
-system restore
-lessons learned

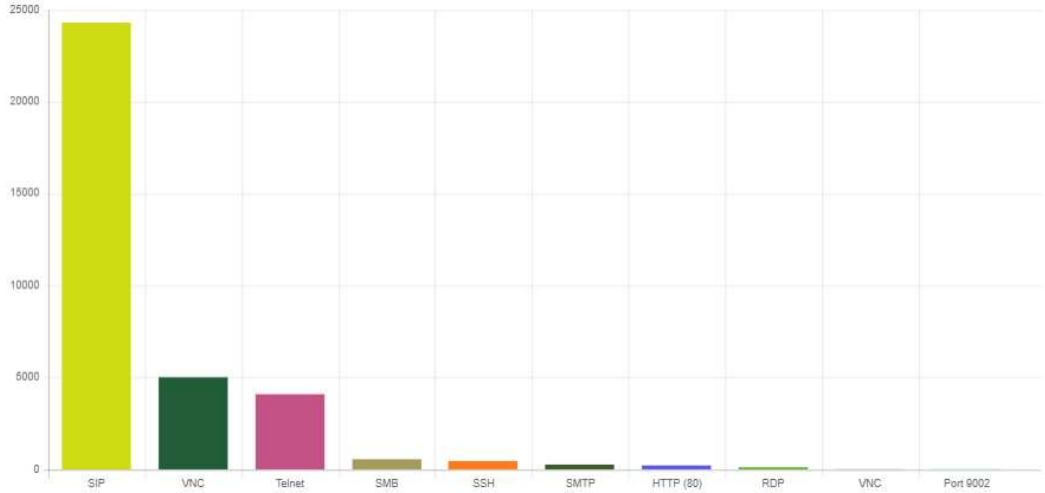


Cert.ro

Evenimente săptămâna 09.09.19 - 15.09.19

În săptămâna 09.09-15.09 se poate observa numărul exagerat de mare al atacurilor către serviciul SIP. Deși aflate la mare distanță, atacurile către serviciile Telnet și VNC au un număr peste media întâlnită până în prezent. Tot săptămâna aceasta se poate observa și apariția portului 9002 care face parte din zona porturilor dinamice.

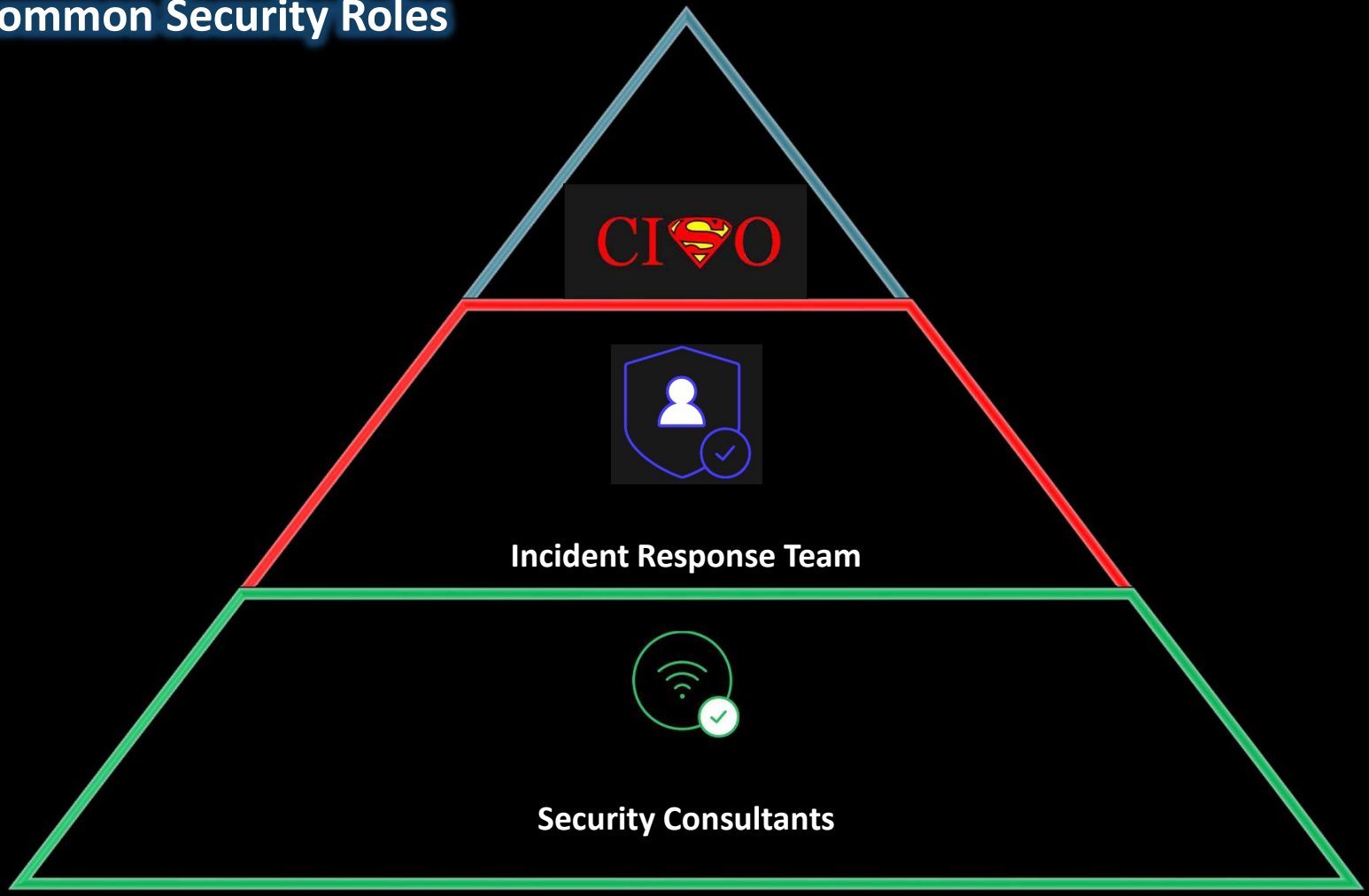
Cele mai atacate servicii



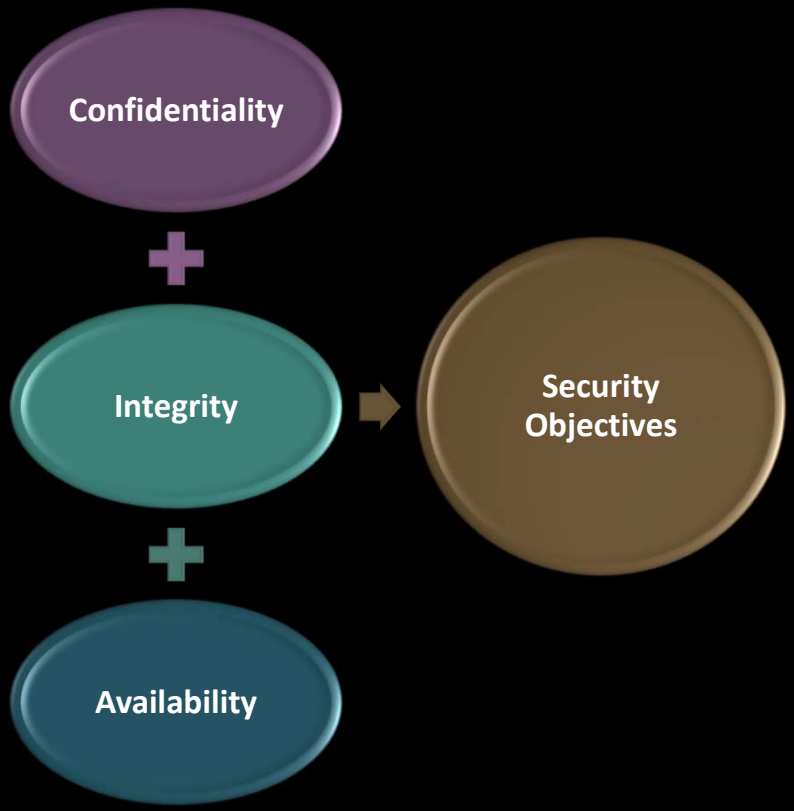
Cele mai încercate nume de utilizator

Cele mai încercate parole

Most common Security Roles



CIA Triad

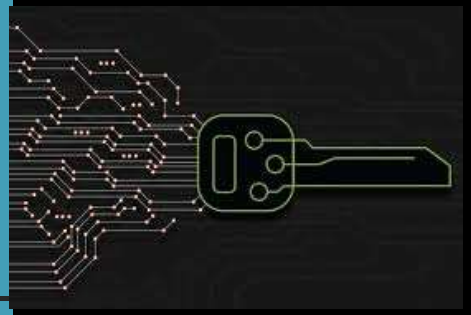


The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts.

—Eugene H. Spafford

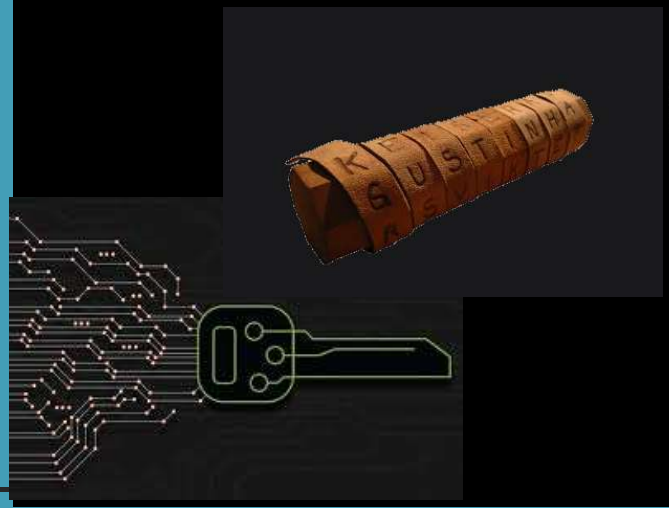
Confidentiality

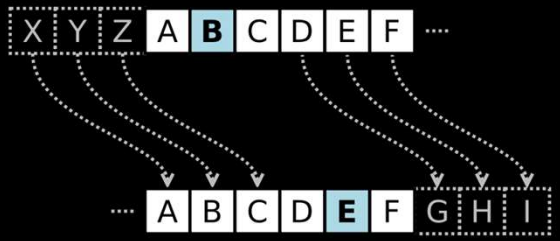
- Ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them.
- It is implemented through security mechanisms such as usernames, passwords, access control lists (ACLs), and encryption.
- The level of secrecy should prevail while data resides on systems and devices within the network, as it is transmitted, and once it reaches its destination
- Attackers can thwart confidentiality mechanisms by network monitoring, shoulder surfing, stealing password files, breaking encryption schemes, and social engineering

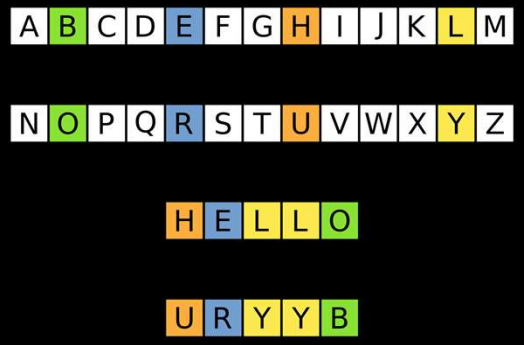


Cryptography

- Is a method of storing and transmitting data in a form that only those it is intended for can read and process
- It is considered a science of protecting information by encoding it into an unreadable format
- Old cryptographic techniques includes: Scytale cipher, Caesar cypher , ROT13
- With enough time, resources, and motivation, hackers can successfully attack most cryptosystems and reveal the encoded information.

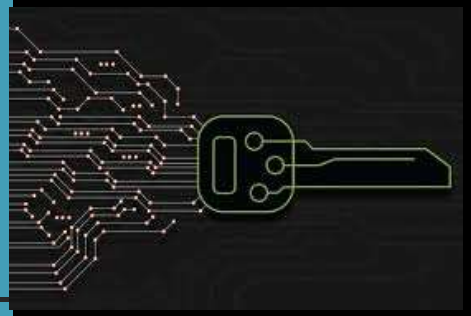


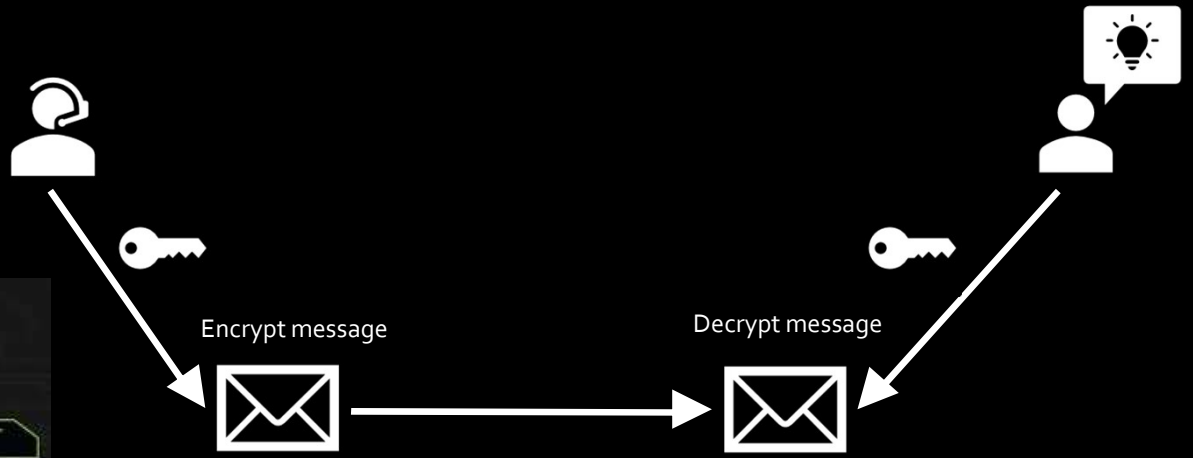




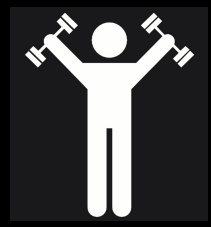
Symmetric Cryptography

- The sender and receiver use the same key for encryption and decryption
- The security of the symmetric encryption method is completely dependent on how well users protect the key
- The key must be shared through an *out-of-band method.*
- Because both users employ the same key to encrypt and decrypt messages, symmetric cryptosystems can provide confidentiality, but they cannot provide authentication or nonrepudiation





Symmetric Cryptography

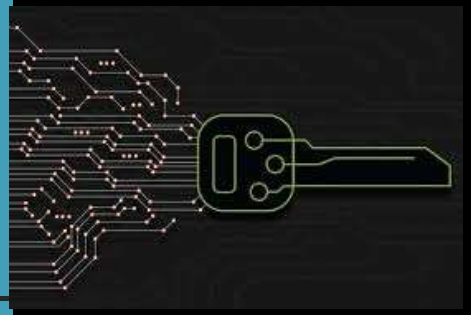


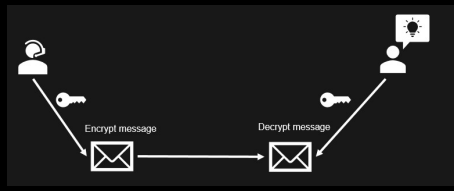
Strengths:

- Much faster (less computationally intensive) than asymmetric systems.
- Hard to break if using a large key size.

Weaknesses:

- Requires a secure mechanism to deliver keys properly.
- Provides confidentiality but not authenticity or nonrepudiation.
- Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming.





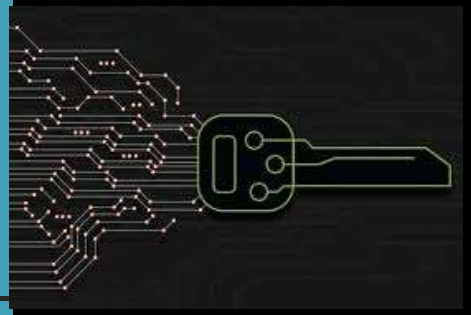
Symmetric Cryptography

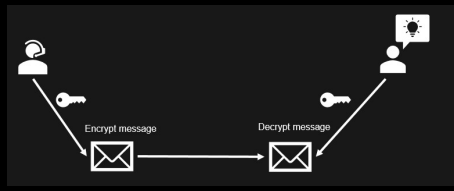
Examples of symmetric algorithms

- Data Encryption Standard (DES) -Has been used since the mid-1970s.
  -It was the primary standard used in government and industry until it was replaced by AES.
  -It's based on a 56-bit key
  -It is now considered insecure because of the small key size.

- Triple-DES (3DES) -Is a technological upgrade of DES.
  -It increases the key length to 168 bits (using three 56-bit DES keys).

- Advanced Encryption Standard (AES) -Has replaced DES as the current standard.
  -Is the current product used by U.S. governmental agencies.
  -It supports key sizes of 128, 192, and 256 bits, with 128 bits being the default.





Symmetric Cryptography

Examples of symmetric algorithms

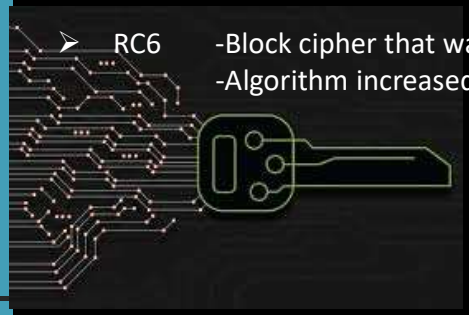
- Blowfish -Performs a 64-bit block cipher at very fast speeds.
  -It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits).
  -Twofish is quite similar and works on 128-bit blocks. The distinctive feature of the latter is that it has a complex key schedule

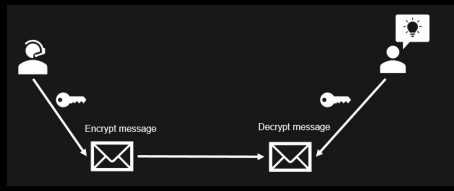
- International Data Encryption Algorithm (IDEA) -Developed by a Swiss consortium. It's an algorithm that uses a 128-bit key.
  -Similar in speed and capability to DES, but it's more secure.

- RC4 -Streaming cipher that works with key sizes between 40 and 2048 bits,.
  -Simple, fast, and efficient,
  -Vulnerable to modification attacks.

- RC5 -Uses block sizes of 32, 64, or 128 bits. The key size goes up to 2,048 bits.
  -The number of rounds can go up to 255.

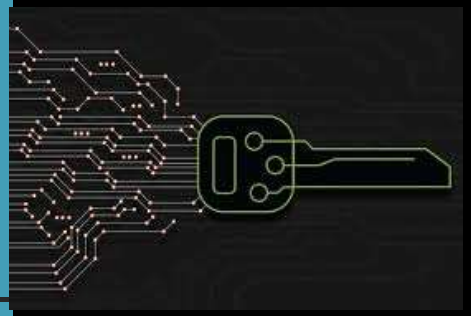
- RC6 -Block cipher that was built upon RC5
  -Algorithm increased the overall speed





Asymmetric Cryptography

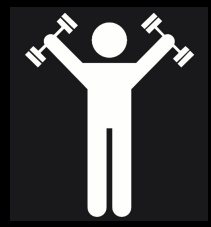
- Are slower than symmetric algorithms because they use much more complex mathematics to carry out their functions, which requires more processing time.
- Can provide authentication and nonrepudiation, depending on the type of algorithm being used.
- Use two keys (public key and the private key) to encrypt and decrypt data.
- The two different asymmetric keys are mathematically related. If a message is encrypted by one key, the other key is required in order to decrypt the message. However, if data is encrypted with a private key, it cannot be decrypted with a private key. If data is encrypted with a private key, it must be decrypted with the corresponding public key.
- The public key can be known to everyone, and the private key must be known and used only by the owner



Asymmetric Cryptography

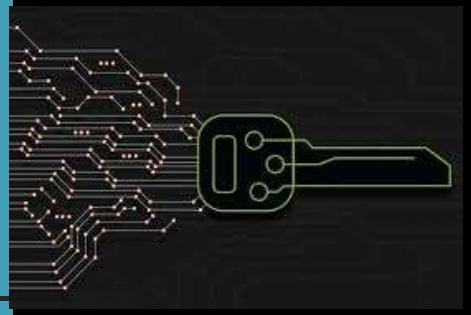
Strengths:

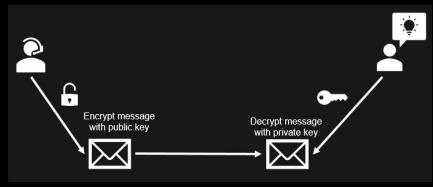
- Better key distribution than symmetric systems.
- Better scalability than symmetric systems.
- Can provide authentication and nonrepudiation.



Weaknesses:

- Works much more slowly than symmetric systems.
- Mathematically intensive tasks.

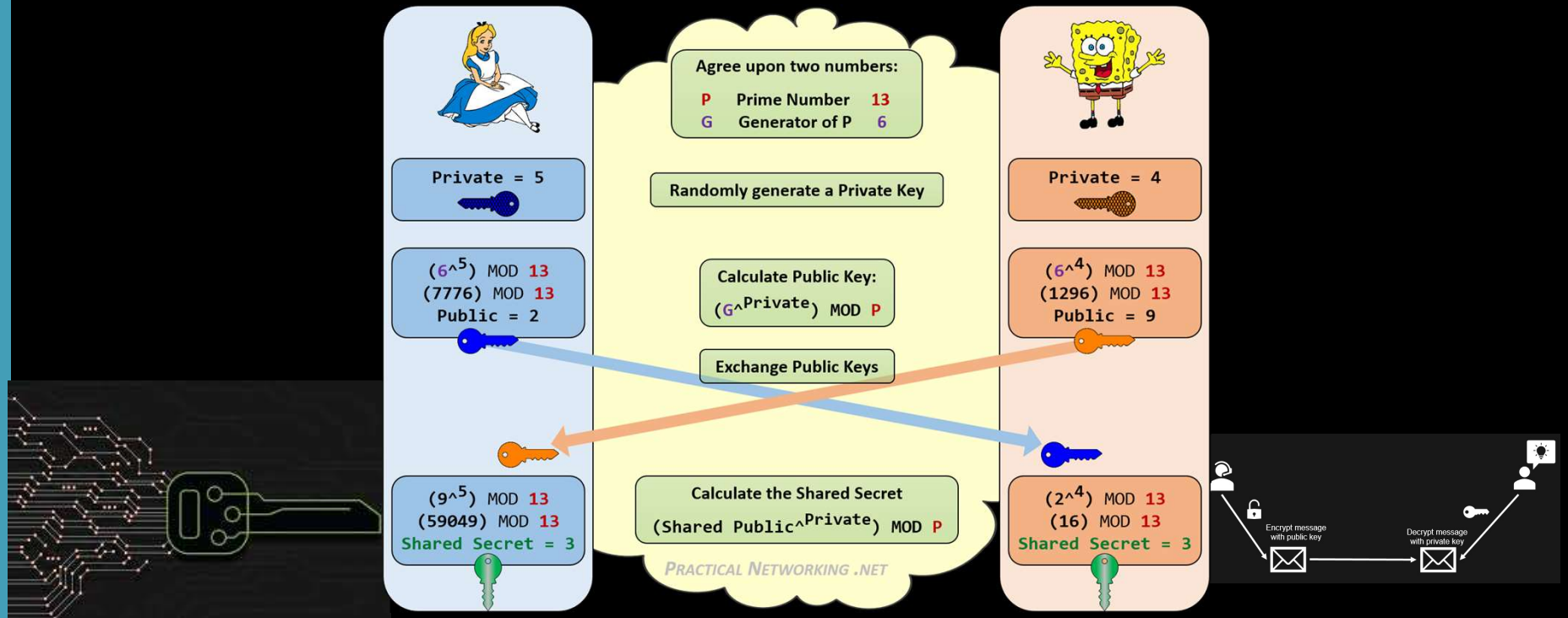




Asymmetric Cryptography

Examples of asymmetric algorithms

- Diffie-Hellman Algorithm- Is used primarily to send keys across public networks. The process isn't used to encrypt or decrypt messages



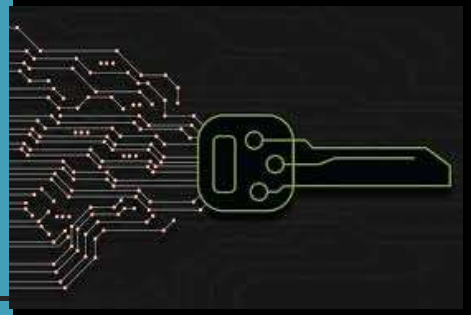
Asymmetric Cryptography

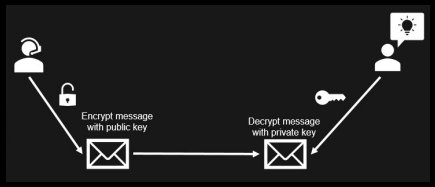
Examples of asymmetric algorithms

- RSA -Can be used for digital signatures, key exchange, and encryption.
  -Developed in 1978 at MIT.
  -The security comes from the difficulty of factoring large numbers into their original prime numbers.

- El Gamal-Can be used for digital signatures, encryption, and key exchange.
  -It is based calculating discrete logarithms in a finite field (if b and g are integers, then k is the logarithm in the equation bk= g.
  -When compared to other algorithms, this algorithm is usually the slowest.

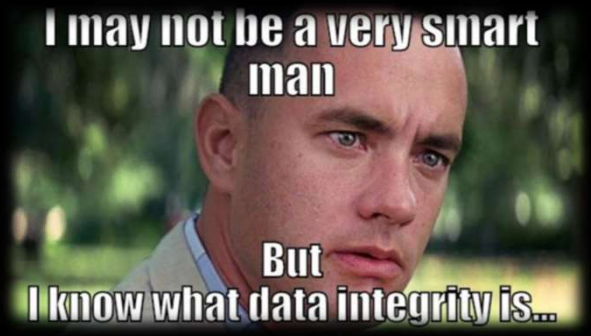
- Elliptic curve cryptosystem (ECC) -Provides much of the same functionality RSA provides: digital signatures, secure key distribution, and encryption.
  -ECC is more efficient than RSA and any other asymmetric algorithm.





Integrity

- The second principle of the CIA Triad
- Protects the reliability and correctness of data
- Prevents unauthorized alterations of data
- Ensures that data remains correct, unaltered, and preserved.
- It protects against malicious unauthorized activities as well as mistakes made by authorized users
- Alterations should not occur while the object is in storage, in transit, or in process.



Integrity

- Prevents unauthorized subjects from making modifications
- Prevents authorized subjects from making unauthorized modifications, such as mistakes
- Maintains the internal and external consistency of objects so that the data is a correct and a true reflection of the real world (protecting the reliability and correctness of data)
- In order to maintain integrity on a system, we must use controls that restrict access to data, objects, and resources.
- Modifying or deleting files, entering invalid data, altering configurations (including errors in commands), introducing a virus, executing malicious code such as a Trojan horse are some examples of integrity breaches

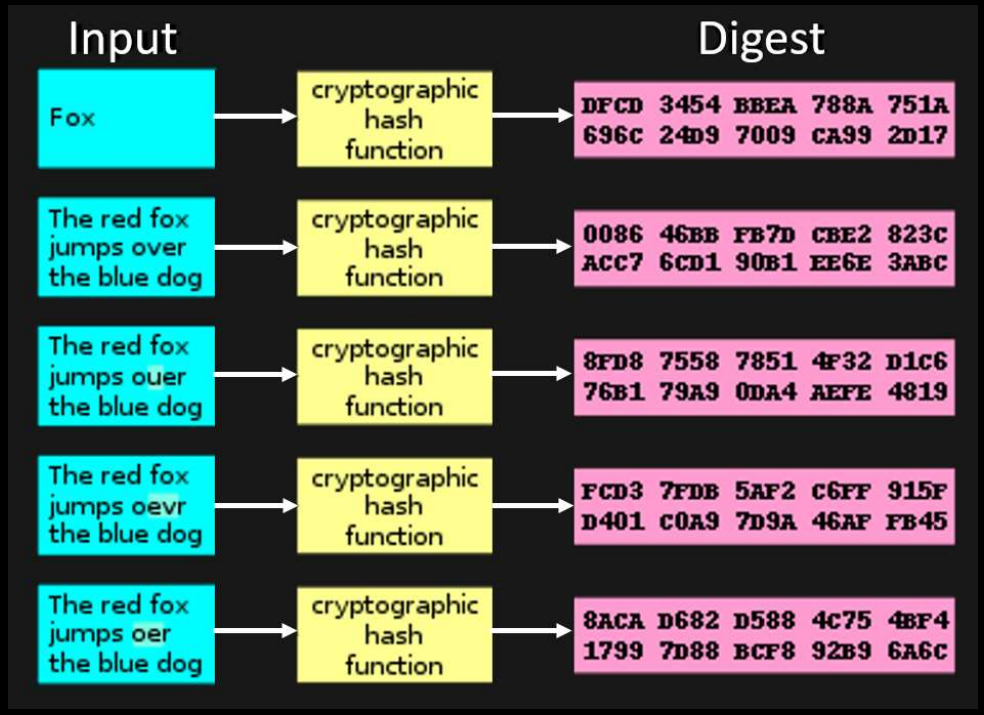
Integrity – Related Concepts

- **Accuracy**: Being correct and precise
- **Authenticity**: Being authentic or genuine
- **Validity**: Being factually or logically sound
- **Accountability**: Being responsible or obligated for actions and results
- **Completeness**: Having all needed and necessary components or parts
- **Comprehensiveness**: Being complete in scope; the full inclusion of all needed elements
- **Nonrepudiation**: Not being able to deny having performed an action or activity or being able to verify the origin of a communication or event

Hashing

- Function that takes a variable-length string (a message) and produces a fixed-length value called a hash value.
- Take a potentially long message and generate a unique output value derived from the content of the message. (message digest)
- The recipient can use the same hash function to recompute the message digest from the full message.
- Compare the message digests: no match =>message was modified
- Messages must be exactly identical for the digests to match

Hashing


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Hashing Algorithms

- MD2 -No longer accepted as suitable hashing functions.

  -Pads the message so that its length is a multiple of 16 bytes. It then computes a 16-byte checksum and appends it to the end of the message. A 128-bit message digest is then generated by using the entire original message along with the appended checksum.

- MD4 -Pads the message to ensure that the message length is 64 bits smaller than a multiple of 512 bits. The MD4 algorithm then processes 512-bit blocks of the message in three rounds of computation. The final output is a 128-bit message digest

- MD5 -It also processes 512-bit blocks of the message

  -It uses four distinct rounds of computation to produce a digest of the

  -Same length as the MD2 and MD4 algorithms (128 bits).

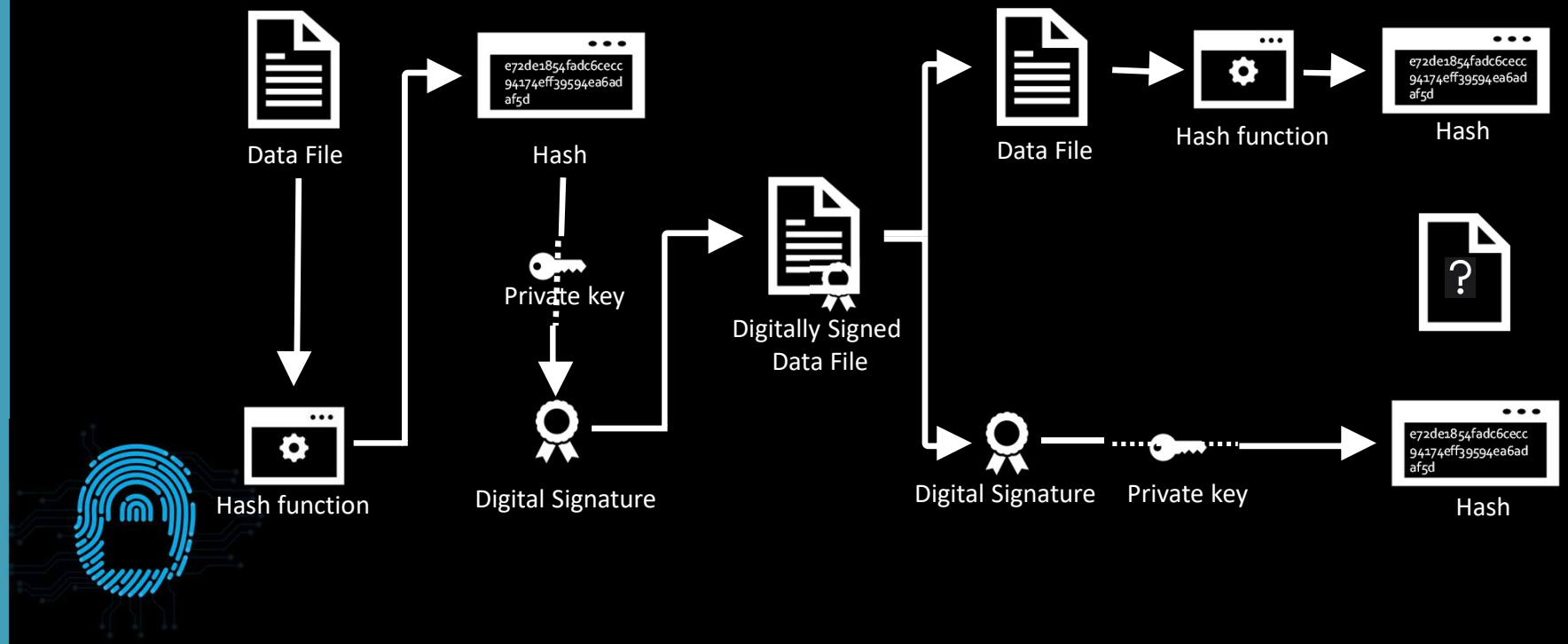
  -Has the same padding requirements as MD4--the message length must be 64 bits less than a multiple of 512 bits.

Hashing Algorithms

- Secure Hash Algorithm (SHA) Produces a 160-bit message digest. It is used with Digital Signature Algorithm (DSA)
- SHA-1 -Takes an input of virtually any length and produces a 160-bit message digest. The algorithm processes a message in 512-bit blocks.
- SHA-256: 256-bit message digest using a 512-bit block size.
- SHA-224: 224-bit message digest using a 512-bit block size.
- SHA-512: 512-bit message digest using a 1,024-bit block size
- SHA-384: 384-bit message digest using a 1,024-bit block size.

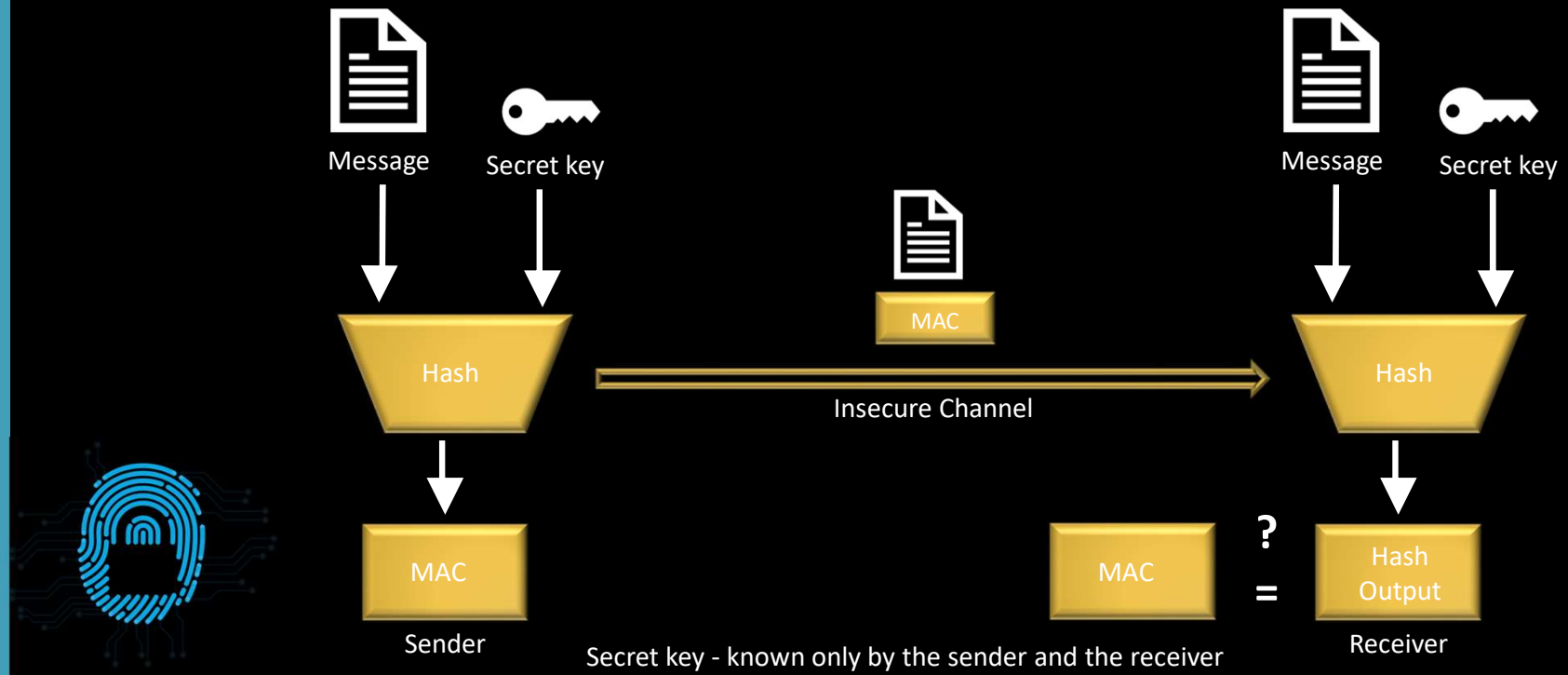
Digital Signatures

- Proves that the message was not changed
- Proves the source of the message



HMAC (Hash Message Authentication Code)

- Combine a hash with a secret key
- Verify data integrity and authenticity
- Used in network encryption protocols e.g. IPsec



Availability

- Third principle of the CIA Triad
- Authorized subjects are granted timely and uninterrupted access to specific objects
- Prevention of DoS & DDoS attacks
- Supporting infrastructure: functional and allows authorized users to gain authorized access.

Availability – Related Concepts

Usability: being easy to use or learn or being able to be understood and controlled by a subject

Accessibility: The assurance that the widest range of subjects can interact with a resource regardless of their capabilities or limitations

Timeliness: Being prompt, on time, within a reasonable time frame, or providing low-latency response

Availability – Threats

Redundant Array of Independent Disks

- **Software Based RAID** -built into your operating system& it all runs on software

  -don't need any special hard drive controllers or any special hardware

- **Hardware based RAID** -we've taken the operating system completely out of the equation

  -we're adding a piece of hardware to our computer.

  -hardware might be built on the motherboard or it might be a separate adapter card

  -the drives directly connect to this hardware.

Redundant Array of Independent Disks

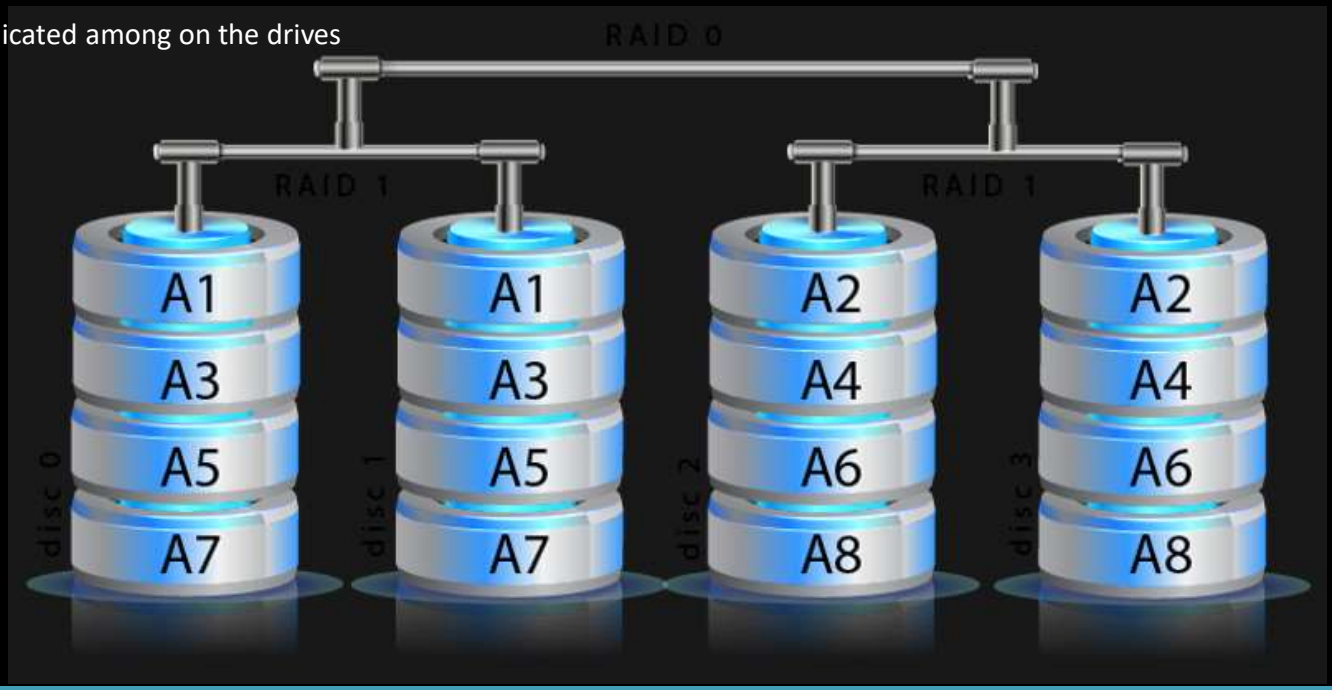
RAID 0 (Striping)

- Take our information, we split it up into different pieces, and we layer it across multiple physical drives.
- We need at least two physical drives to be able to do this

Redundant Array of Independent Disks

RAID 1(Mirroring) /RAID 10

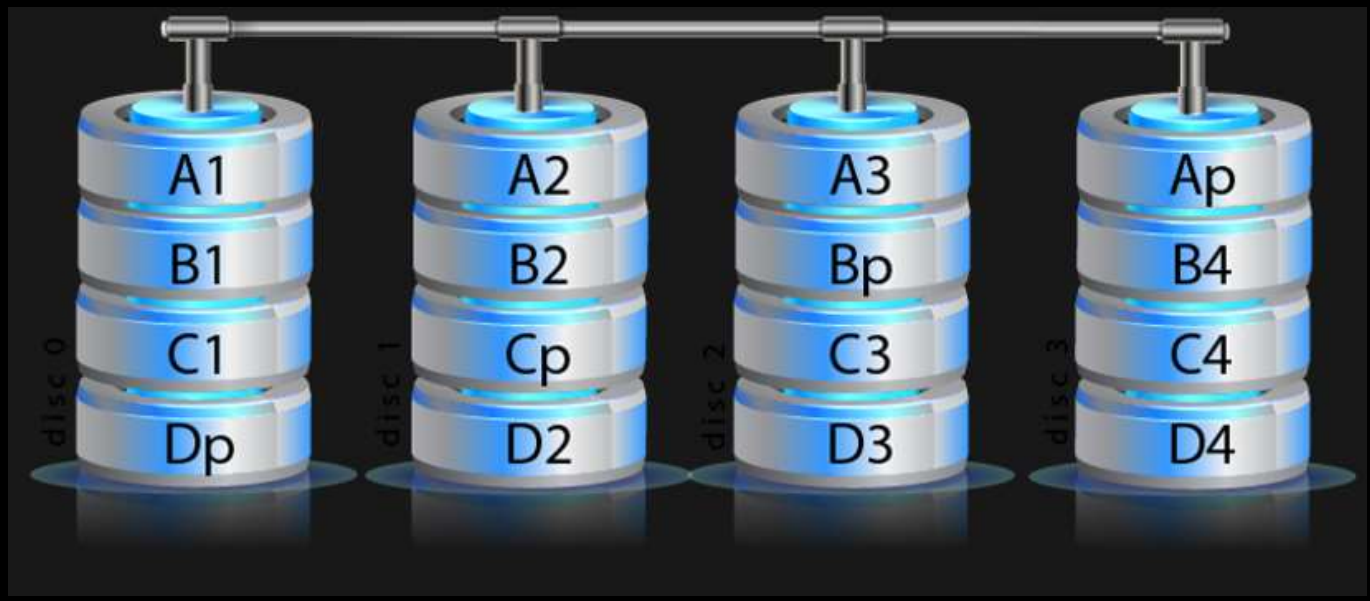
- Create an exact duplicate of the data.
- We need at least two physical drives to be able to do this
- Information is duplicated among on the drives



Redundant Array of Independent Disks

RAID 5

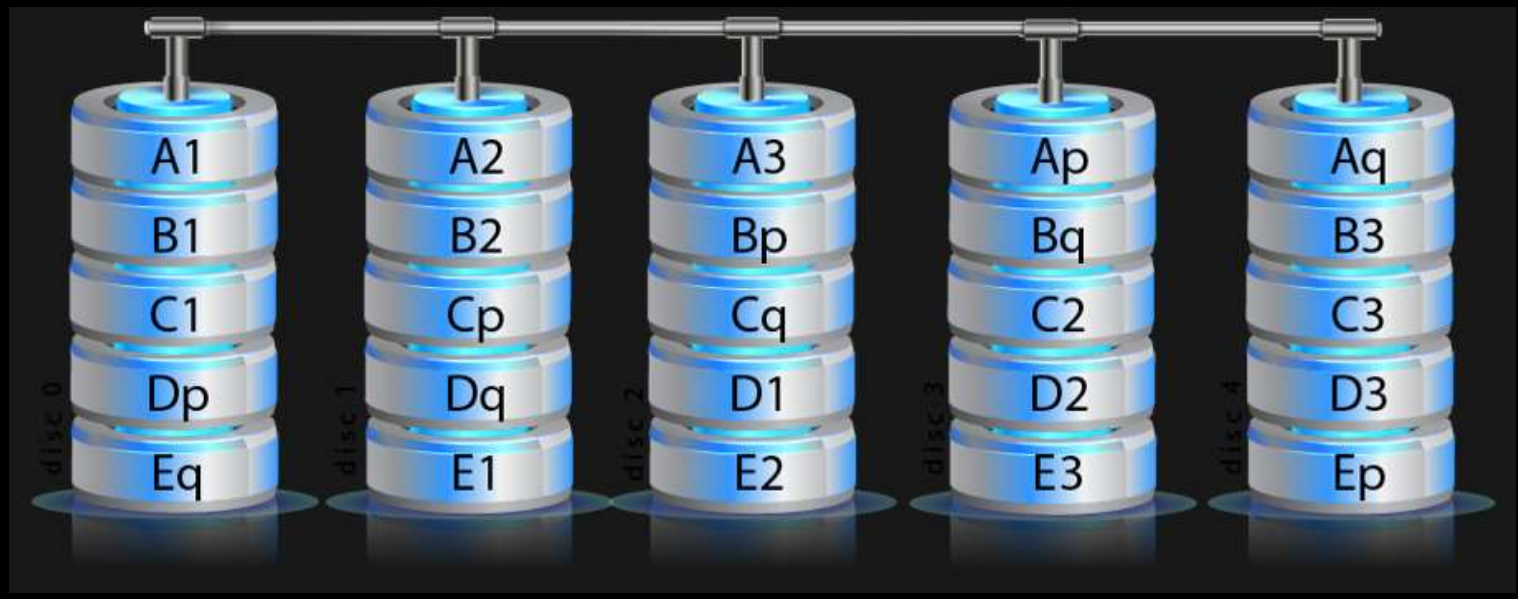
- Uses the striping from RAID 0 but adds a new piece of information called a parity bit to the data
- We're striping this information across multiple disks and we need at least 3 physical disks to be able to use RAID 5.



Redundant Array of Independent Disks

RAID 6

- **H**as distributed parity like a RAID 5, but has an additional parity stripe dedicated to higher fault tolerance
- Two drives could fail without data loss



Redundancy & Backup

- **Redundancy** is an operational requirement of the data center that refers to the duplication of certain components or functions of a system so that if they fail or need to be taken down for maintenance, others can take over.

- Redundant components can exist in any data center system, including cabling, servers, switches, fans, power and cooling.