Security Fundamentals Based on Security+

Hello!

I am Green Timothy

Cybersecurity Expert,
Penetration Tester &
Trainer.

CompTIA Sec+ ,ISC2

You can find me at:

Linkedin:
https://www.linkedin.com/in/green-timothy-91526319a/

Part 5 .
Risk Management

Business Partnership Agreement (BPA)

A legal agreement between partners that establishes the terms, conditions, and expectations of the relationship between the partners

- The sharing of profits and losses
- The responsibilities of each partner

Service Level Agreement (SLA)

A contract between a service provider and a customer that specifies the nature of the service to be provided and the level of service that the provider will offer to the customer

- Technical and performance parameters, such as response time and uptime

Memorandum of Understanding (MOU)
Memorandum of Agreement (MOA)

An agreement expressing a set of intended actions between the parties with respect to some common goal.

- Does not need to contain legally enforceable promises but It can be based on the intent of the parties.

Interconnection security agreement (ISA):

An agreement between organizations that have connected or shared IT systems.

- ISA explains the security controls in place to protect the confidentiality, integrity, and availability of the systems and associated data

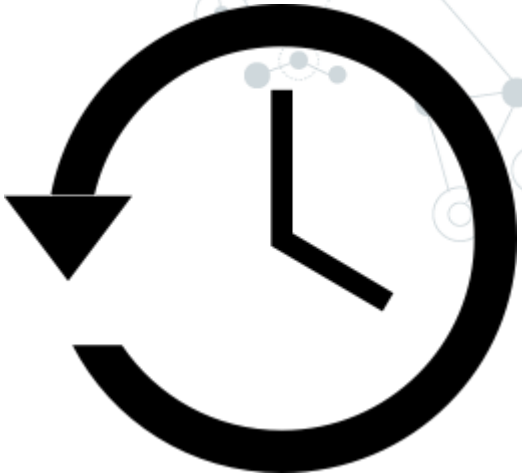
Non-disclosure agreement (NDA)

a legal contract between at least two parties that share with one another confidential material for certain purposes, but wish to restrict access to or by third parties

Business Impact Analysis (BIA)

- A process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency.

Recovery Time Objective (RTO)



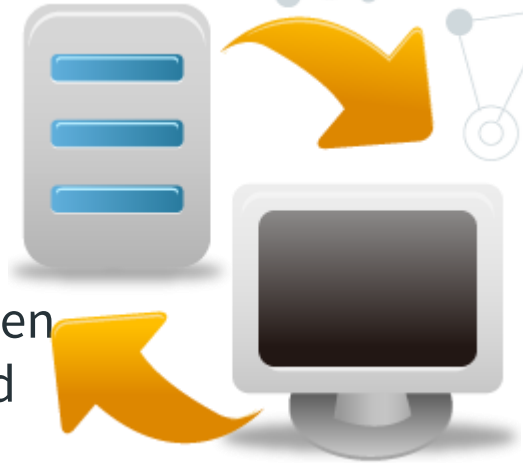
The target time you set for the recovery of your IT and business activities after a disaster has occurred

- This is a period of time that is defined based on the needs of the business (Ex: 5 hours RTO)
- A shorter RTO results in higher costs because it requires greater coordination and resources

- "How much time did it take to recover after notification of business process disruption?"

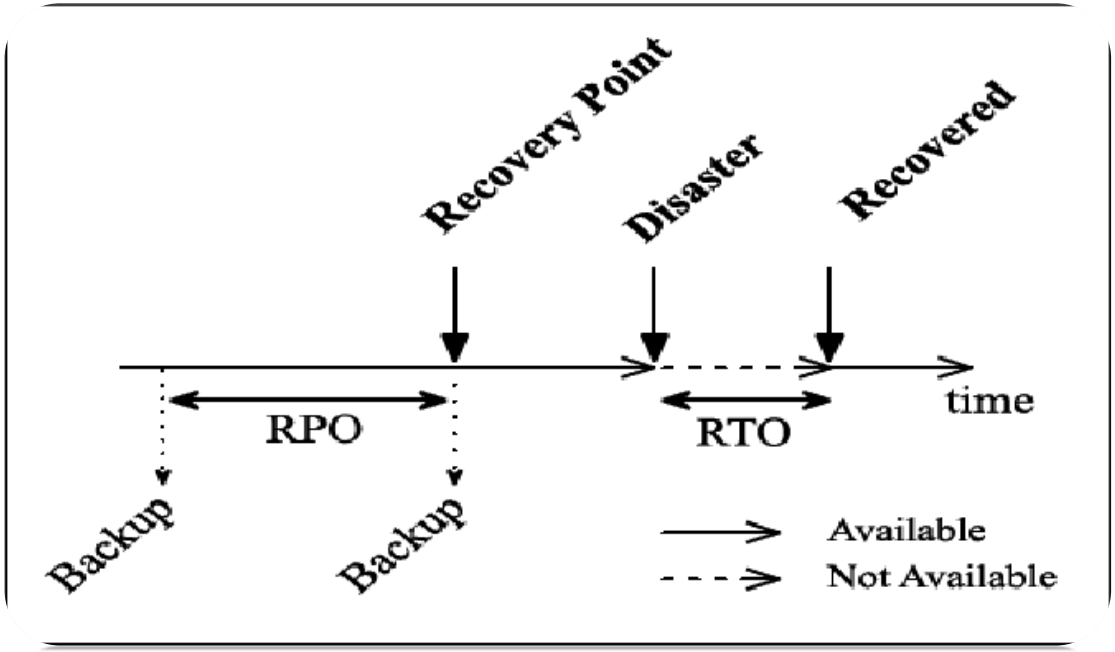
Recovery Point Objective (RPO)

RPO focused on data and your company's loss tolerance in relation to your data



- RPO is determined by looking at the time between data backups and the amount of data that could be lost in between backups

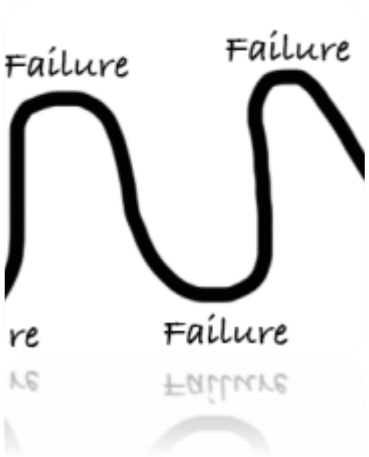
- Ex : Imaging that you are writing a, report. And you know eventually your computer will crash and the content written after your last save will be lost. How much time can you tolerate having to try to recover, or rewrite that missing content


Recovery Point
Disaster
Recovered
time
RPO
RTO
Backup
Backup
Available
Not Available

Mean time between failures (MTBF)

The average amount of time that passes between hardware component failures

- Used for products that can be repaired and returned to use
- Can be predicted based on product experience or data supplied by the manufacturer



Mean time To failure (MTTF)

The time a device or product is expected to last in operation

- MTTF is used for nonrepairable products.
- Based experience or by the manufacturer

Mean time To restore/repair (MTTR)

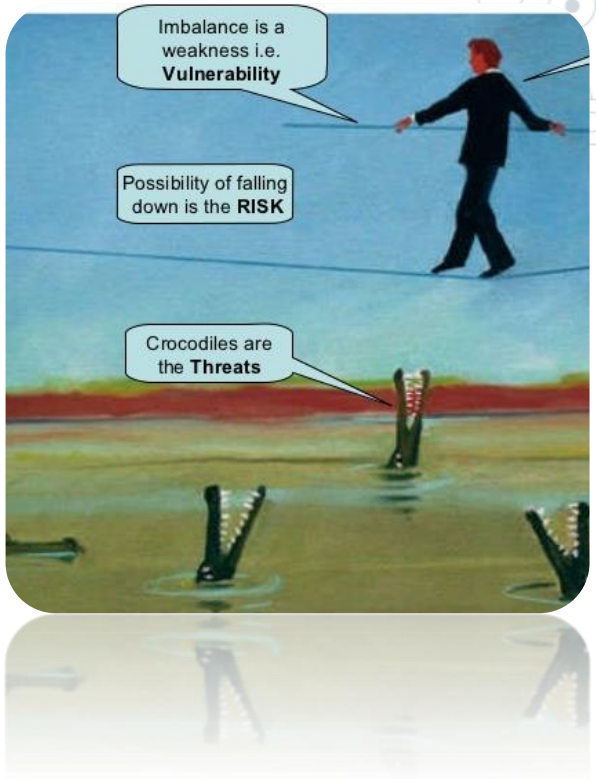
The average time required to fix a failed component or device and return it to production status

RISK MANAGEMENT

The process of identifying and reducing risk to a level that is acceptable and then implementing controls to maintain that level

- Threat is Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset
- Vulnerability is a weakness or gap in our protection efforts.
- Risk is The possibility of or exposure to loss or danger

Risk = Threat X Vulnerability



Threat Assessment

Analysis of the threats that confront an enterprise

- generally cannot change the threat—you can only change how it affects you

Environmental threats

- Tornado, hurricane, earthquake, severe weather

Man-made threats

- Internal threats are from employees (remove files)
- External threats are from outside the organizations (Attackers)

Quantitative risk assessment

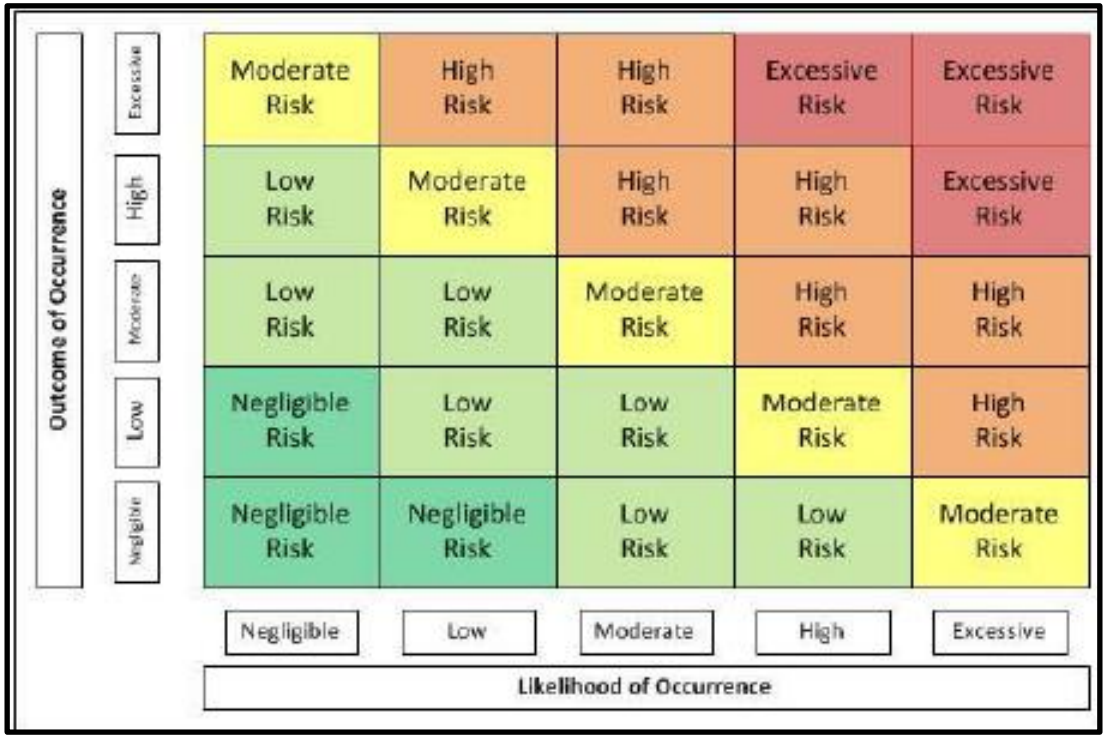
Quantitative measures give the clearest measure of relative risk and expected return on investment

- Quantitative (think quantity) is expressed numerically

Qualitative risk assessment

Can involve brainstorming, focus groups, surveys, and other similar processes

Qualitative (think quality) is expressed as “High” or “Low.”


Outcome of Occurrence
Excessive
High
Moderate
Low
Negligible
Moderate Risk
High Risk
High Risk
Excessive Risk
Excessive Risk
Low Risk
Moderate Risk
High Risk
High Risk
Excessive Risk
Low Risk
Low Risk
Moderate Risk
High Risk
High Risk
Negligible Risk
Low Risk
Low Risk
Moderate Risk
High Risk
Negligible Risk
Negligible Risk
Low Risk
Low Risk
Moderate Risk
Negligible
Low
Moderate
High
Excessive
Likelihood of Occurrence

Annualized Rate of Occurrence (ARO)

How likely is it that a DDoS will hit in a year?

- Quantitative (think quantity) is expressed numerically

Single Loss Expectancy (SLE)

What is the monetary loss if a single event occurs?

- Laptop stolen (asset value) = $1,000

Annual Loss Expectancy (ALE)

- ALE = ARO x SLE
- 7 laptops stolen a year (ARO) x $1,000 (SLE) = $7,000

Risk response techniques

Risk-avoidance

- Stop participating in high-risk activity

Transference

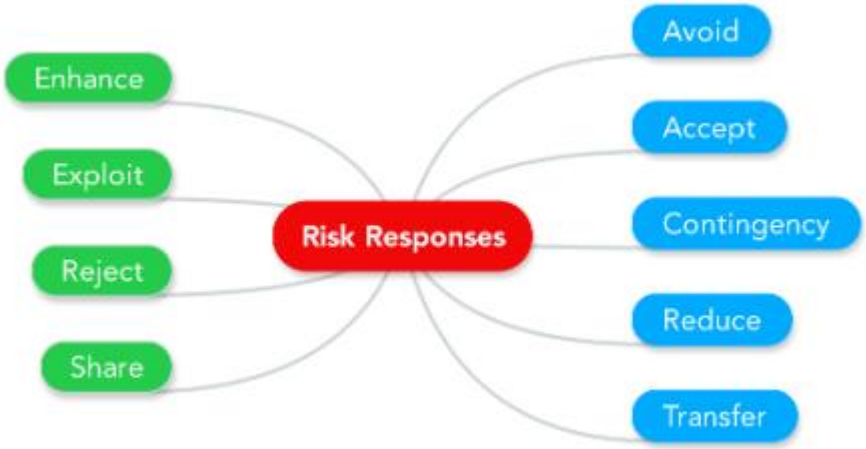
- Buy some insurance

Acceptance

- A business decision;
- we'll take the risk!

Mitigation

- Reduce the risk level
- Invest in security systems



Incident Response Planning

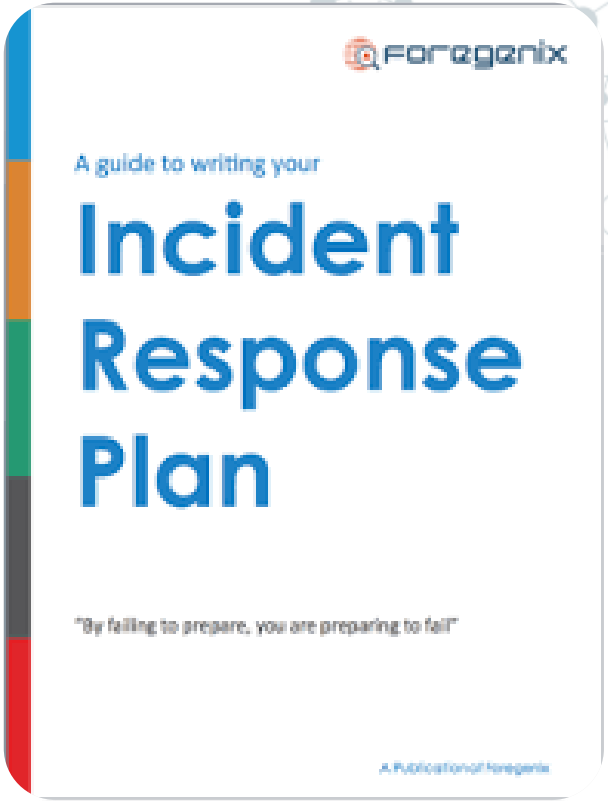
The steps an organization performs in response to any situation determined to be abnormal in the operation of a computer system.

Security incidents categories

- Email Phishing Attack
- Improper usage
- Attack resulted from a violation of the
- Loss or theft of equipment

Roles and responsibilities

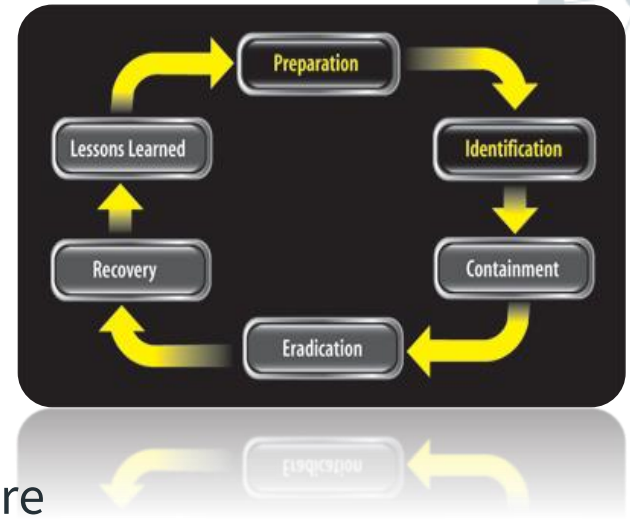
- Incident response team
- IT security management
- External contacts



Incident Response Process

The set of actions security personnel perform in response to a wide range of triggering events.

- NIST Special Publication 800-61
- Computer Security Incident Handling Guide



Preparing

- Communication methods
- Incident handling hardware and software
- Incident analysis resources
- Documentation, network diagrams
- critical file hash values
- Clean OS and application images
- Policies needed for incident handling

Identification and Analysis

In this process you need to work out whether you are dealing with an event or an incident.

Containment

Working with the business to limit the damage caused to systems and prevent any further damage from occurring

Eradication

Ensuring you have a clean system ready to res

- Reimage of a system
- a restore from a known good backup

Recovery

Determine when to bring the system back in to production and how long we monitor the system for any signs of abnormal activity.

Lessons Learned

- Invite everyone affected by the incident
- Some recommendations can be applied
- to the next event

Part 6 .
Cryptography

Cryptography

- The process of converting readable data (called plaintext) into unreadable text

Plaintext

- An unencrypted message (in the clear)

Ciphertext

- An encrypted message

Cipher

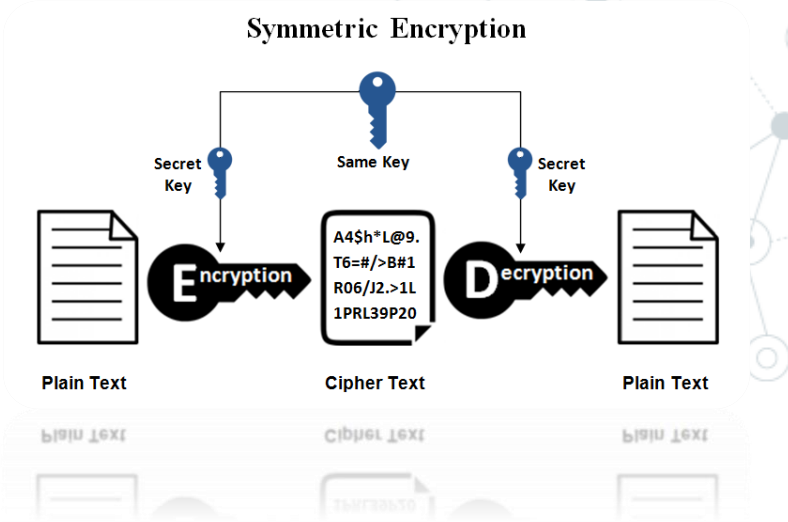
- The algorithm used to encrypt and/or decrypt

Cryptanalysis

- The art of cracking encryptions

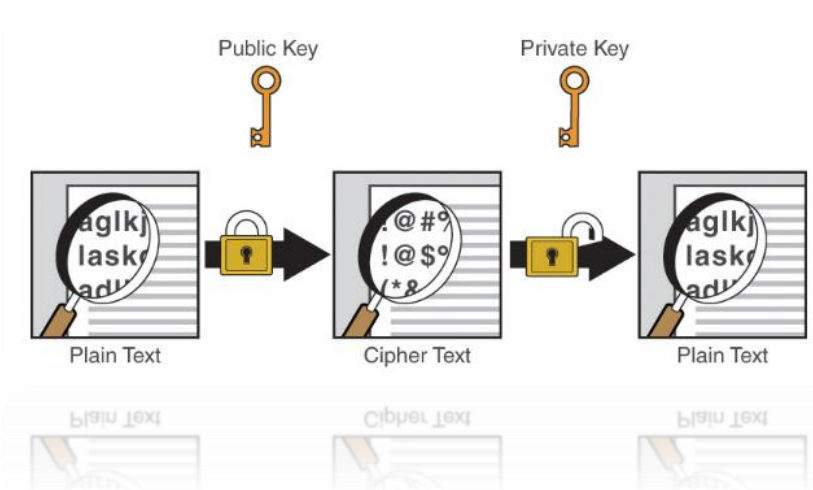
Symmetric encryption

- A single, shared key
- Encrypt with the key
- Decrypt with the same key
- If it gets out, you'll need another key
- 128-bit or larger symmetric keys are common



A Symmetric encryption

- Private key (Keep this private)
- Public key (Anyone can see this key)



Symmetric Algorithms

AES (Advanced Encryption Standards)

- 128-, 192-, and 256-bit keys
- Used in WPA2 - Powerful wireless encryption

DES and 3DES (Data Encryption Standard)

- 56-bit key (Easy to brute force)
- Today we have 3DES that uses three keys with 56 bits each. The total key length = 168 bits

A Symmetric Algorithms

- Diffie-Hellman key exchange
- RSA
- PGP (Pretty Good Privacy)

Stream ciphers

- Used only with symmetric encryption
- Encryption is done one bit or byte at a time
- High speed, low hardware complexity

Block ciphers

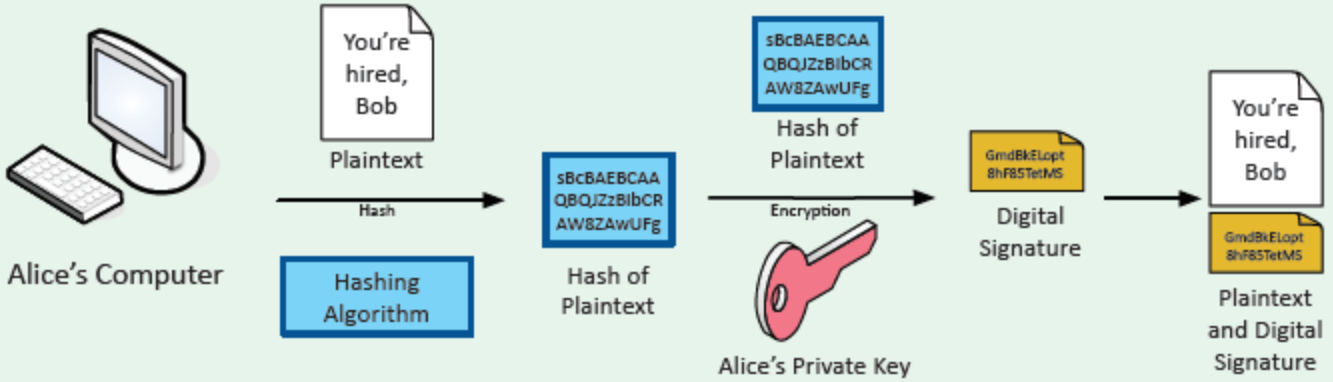
- Used with Symmetric and Asymmertric
- Encrypt fixed-length groups
- Often 64-bit or 128-bit blocks
- Pad added to short blocks
- Each block is encrypted or decrypted independently

Digital signatures

- Prove the message was not changed
  Integrity
- Prove the source of the message
  Authentication
- Make sure the signature isn't fake
  Non-repudiation

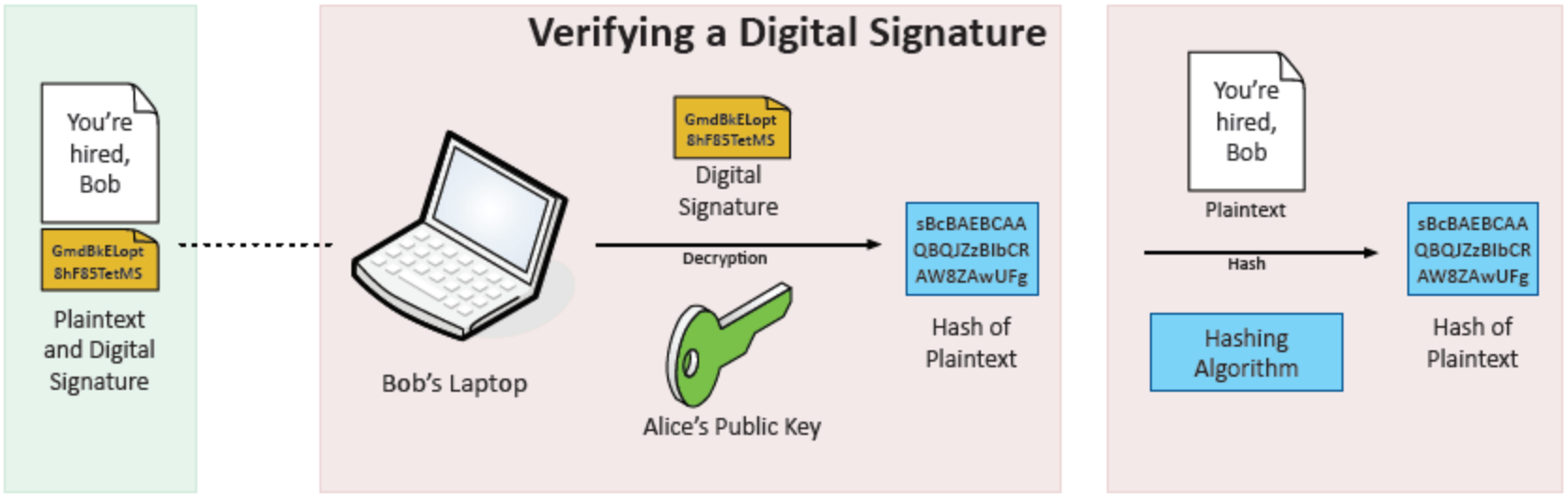
- Sign with his private key
- The message doesn't need to be encrypted
- Verify with the public key
  Any change in the message will invalidate the signature

Creating a Digital Signature



1. Alice creates a hash of the original plaintext
2. Alice encrypts the hash with her private key
3. The encrypted hash (digital signature) is included with the plaintext

Verifying a Digital Signature



1. Bob decrypts the digital signature to obtain the plaintext hash
2. Bob hashes the plaintext and compares it to the decrypted hash

Data in-transit (In Motion)

- Data transmitted over the network
- Network-based protection - Firewall, IPS
- TLS (Transport Layer Security)
- IPsec (Internet Protocol Security)

Data at-rest

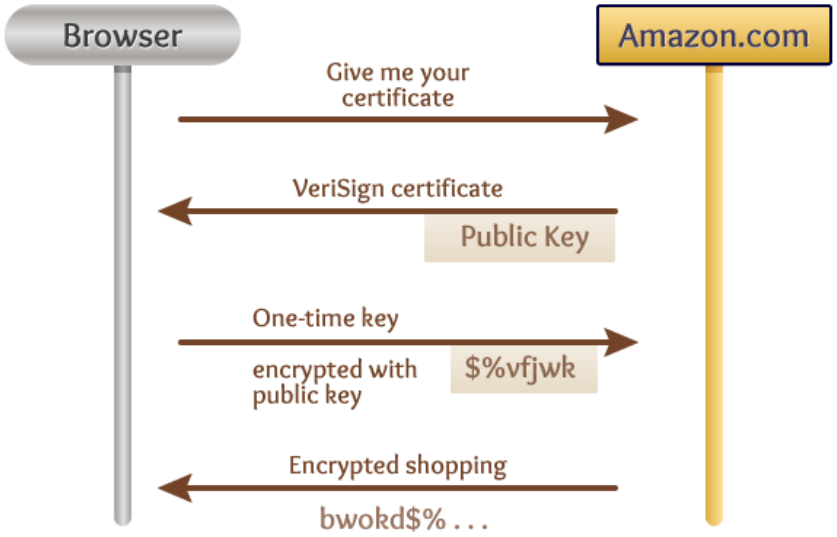
- Hard drive, SSD, flash drive, etc.
- Use disk encryption, database encryption
- File- or folder-level encryption

Data in use

- System RAM, CPU registers and cache
- The data is almost always decrypted
- Otherwise, you couldn't do anything with it

Encrypting HTTPS traffic SSL/TLS

- Client requests secure session
- Server sends its certificate including its public key
- The client creates a symmetric key and encrypts it with the servers public key
- The client sends the encrypted symmetric key to the server
- The server decrypts the symmetric key using its private key
- All of the session data from thereon is encrypted with the symmetric key



Time for Testing ourselves and answering some questions!