Welcome to the third CBK Domain.

In this domain we cover:

The domain has 3 major knowledge areas (prior to the 2015 exam update, each had their own domain).

- **Security Architecture and Design**
  - The common security models
  - The architecture, design, virtualization, cloud and solutions we use to protect our assets
  - How computers work (basic), and how they are logically segmented.
  - Threats to our applications, systems and devices
- **Cryptography**
  - The common security models
  - The architecture, design, virtualization, cloud and solutions we use to protect our assets
  - How computers work (basic), and how they are logically segmented.
  - Threats to our applications, systems and devices
- **Physical Security**
  - Site and facility secure design principles, perimeter defense, HVAC, power, fire suppression

CBK 3 makes up 13% of the exam questions, being so broad it contains close to 25% of the exam materials.

Security Architecture and Design

- **Security Models Fundamental Concepts:**
  - Security models provide the rules for how we secure our data, while focusing on different goals and what they provide.
  - **DAC** - (Discretionary Access Control) gives subjects full control of objects they have created or been given access to.
  - **MAC** - (Mandatory Access Control) is system-enforced access control based on a subject's clearance and an object's labels.
  - **RBAC** - (Role Based Access Control) is where access to objects is granted based on the role of the subject.
  - **ABAC** - (Attribute Based Access Control) is where access to objects is granted based on subjects, objects, and environmental conditions.
    - Attributes could be:
      - *Subject* (user) – Name, role, ID, clearance, etc.
      - *Object* (resource) – Name, owner, and date of creation.
      - *Environment* – Location, and/or time of access, and threat levels.

- **RUBAC** - (Rule Based Access Control) is access that's granted based on IF/THEN statements.

- **Bell-LaPadula: (Confidentiality)** (Mandatory Access Control):
  - **Simple Security Property** "No Read UP".
    - Subjects with Secret clearance can't read Top Secret data.

  - *** Security Property:** "No Write DOWN".
    - Subjects with Top Secret clearance can't write Top Secret information to Secret folders.

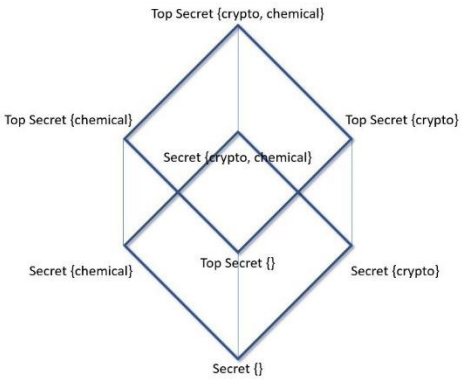
  - **Strong * Property:** "No Read or Write UP and DOWN".
    - Subjects can ONLY access data on their own level.

- **BIBA: Integrity** (Mandatory Access Control):
  - **Simple Integrity Axiom:** "No Read DOWN".
    - Subjects with Top Secret clearance can't read Secret data.
    - Remember that integrity is the purpose here; we don't want to have wrong or lacking lower clearance level data confuse us.

  - *** Integrity Axiom:** "No Write UP".
    - Subjects with Secret clearance can't write Secret information to Top Secret folders.
    - We don't want wrong or lacking lower level information to propagate to a higher level.

  - **Invocation Property:** "No Read or Write UP".
    - Subjects can never access or alter data on a higher level.

- **Lattice Based Access Control (LBAC) (MAC):**
  - A subject can have multiple access rights.
    - A Subject with "Top Secret" {crypto, chemical} would be able to access everything in this lattice.
    - A Subject with "Secret" {crypto} would only have access to that level.
    - A subject with "Top Secret" {chemical} would have access to only {chemical} in Top Secret and Secret.
  - These are obviously vastly more complex in real life.
  - For the exam, just know what they are and how they work.

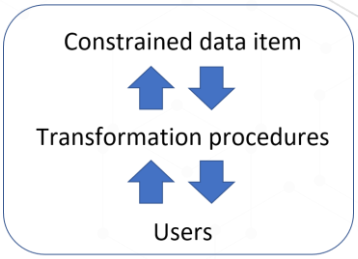


  - We will cover Access Models more in depth in Domain 5.

- **Graham-Denning Model** – uses Objects, Subjects, and Rules.
  - The 8 rules that a specific subject can execute on an object are:
    1. Transfer Access.
    2. Grant Access.
    3. Delete Access.
    4. Read Object.
    5. Create Object.
    6. Destroy Object.
    7. Create Subject.
    8. Destroy Subject.

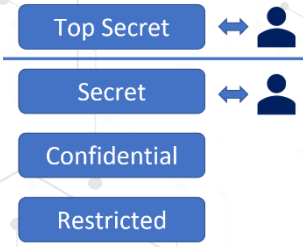
- **HRU** model (Harrison, Ruzzo, Ullman):
  - An operating system level computer security model that deals with the integrity of access rights in the system.
  - It is an extension of the Graham-Denning model, based around the idea of a finite set of procedures being available to edit the access rights of a subject on an object.
  - Considers Subjects to be Objects too (unlike Graham-Denning).
  - Uses six primitive operations:
    - Create object.
    - Create subject.
    - Destroy subject.
    - Destroy object.
    - Enter right into access matrix.
    - Delete right from access matrix.

- **Clark-Wilson - Integrity:**
  - Separates end users from the back-end data through 'Well-formed transactions' and 'Separation of Duties'.
  - The model uses Subject/Program/Object.
    - We have discussed the Subject/Object relationship before, but this puts a program between the two.
    - We don't allow people access to our inventory when they buy from us.
    - We give them a limited functionality interface they can access.

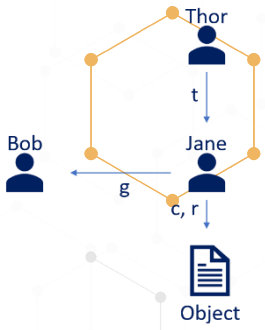


  - **Separation of duties:**
    - The certifier of a transaction and the implementer are different entities.
    - The person making purchase orders should not be paying the invoices.
  - **Well-formed transactions** are a series of operations that transition a system from one consistent state to another consistent state.

- **Brewer-Nash** (Chinese Wall or Information Barriers):
  - Designed to provide controls that mitigate conflict of interest in commercial organizations, and is built upon an information flow model.
  - No information can flow between the subjects and objects in a way that would create a conflict of interest.
- **Non-Interference Model:**
  - Ensures that any actions that take place at a higher security level do not affect, or interfere with actions that take place at a lower level.
  - The model is not concerned with data flow, but with what a subject knows about the state of the system.
  - Any changer by a higher-level subject will never be noticed by a lower level subject.



- **Take-Grant** Protection Model:
  - Uses rules that govern the interactions between subjects and objects.
  - It uses permissions that subjects can grant to (or take from) other subjects.
  - It has 4 rules:
    - **Take** rule allows a subject to take rights of another object.
    - **Grant** rule allows a subject to grant own rights to another object.
    - **Create** rule allows a subject to create new objects.



- **Remove** rule allows a subject to remove rights it has over another object.
  - Thor can Take (t) Jane's rights for the object.
  - Jane can Create (c) and Remove (r) rules for the object.
  - Jane can Grant (g) any of her rights to Bob.

- **Access Control Matrix:**
  - Model describing the rights of every subject for every object in the system.
  - An access matrix is like an Excel sheet.
    - One row per subject.
    - One column per object.
    - The **rows** are the rights of each subject, each row is called a capability list.
    - The **columns** show the ACL (Access Control List) for each object or application.

Subject/Object	Object #1	Object #2	Object #3
Thor	Read	Read, Write	Full Control
Jane	Full Control	Read	No access
Bob	No Access	Full Control	Read, Write

- **Zachman Framework** (for Enterprise Architecture):
  - Provides six frameworks:
    - What, How, Where, Who, When, and Why.
  - Mapping those frameworks to rules for:
    - Planner, Owner, Designer, Builder, Programmer, and User.

	DATA *What*	FUNCTION *How*	NETWORK *Where*	PEOPLE *Who*	TIME *When*	MOTIVATION *Why*
Objective/Scope (*Contextual*) *→ Role: Planner*	List of Things important in the Business	List of Core Business Processes	List of Business Locations	List of important Organizations	List of Events	List of Business Goals/Strategies
Enterprise Model (*Conceptual*) *→ Role: Owner*	Conceptual Data/ Object Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan
System Model (*Logical*) *→ Role: Designer*	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Technology Model (*Physical*) *→ Role: Builder*	Physical Data/ Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Detailed Representations (*Out of Context*) *→ Role: Programmer*	Data Definitions	Program	Network Architecture	Security Architecture	Timing Definition	Rule Specification
Functioning Enterprise *→ Role: User*	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

- **Security Modes** - can be MAC or DAC (Mandatory or Discretionary Access Control):
  The systems contain information at various levels of security classification.
  - **The mode is determined by:**
    - The type of users who will be directly or indirectly accessing the systems.
    - The type of data, including classification levels, compartments, and categories that are processed on the system.
    - The type of levels of users, their need to know, and formal access approvals that the users will have.
  - **Dedicated security mode** - All users must have:
    - Signed NDA for ALL information on the system.
    - Proper clearance for ALL information on the system.
    - Formal access approval for ALL information on the system.
    - A valid need to know for ALL information on the system.
    - All users can access ALL data (continued).

- **System high security mode** - All users must have:
  - Signed NDA for ALL information on the system.
  - Proper clearance for ALL information on the system.
  - Formal access approval for ALL information on the system.
  - A valid need to know for SOME information on the system.
  - All users can access SOME data, based on their need to know.
- **Compartmented security mode** - All users must have:
  - Signed NDA for ALL information on the system.
  - Proper clearance for ALL information on the system.
  - Formal access approval for SOME information they will access on the system.
  - A valid need to know for SOME information on the system.
  - All users can access SOME data, based on their need to know and formal access approval.
- **Multilevel security mode** - (Controlled Security Mode) - All users must have:
  - Signed NDA for ALL information on the system.
  - Proper clearance for SOME information on the system.
  - Formal access approval for SOME information on the system.
  - A valid need to know for SOME information on the system.
  - All users can access SOME data, based on their need to know, clearance and formal access approval.
- **Compartmented security mode** - All users must have:
  - Signed NDA for ALL information on the system.
  - Proper clearance for ALL information on the system.
  - Formal access approval for SOME information they will access on the system.
  - A valid need to know for SOME information on the system.
  - All users can access SOME data, based on their need to know and formal access approval.
- **Multilevel security mode** - (Controlled Security Mode) - All users must have:
  - Signed NDA for ALL information on the system.
  - Proper clearance for SOME information on the system.
  - Formal access approval for SOME information on the system.
  - A valid need to know for SOME information on the system.
  - All users can access SOME data, based on their need to know, clearance and formal access approval.

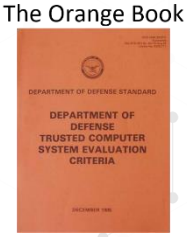
- **Evaluation Methods, Certification and Accreditation:**

  Choosing the security systems and products we implement in our organization can be a daunting task. How do we know the vendor is trustworthy, how do we know the systems and products were tested well and what the tests revealed?

  Rainbow Series

  The Orange Book

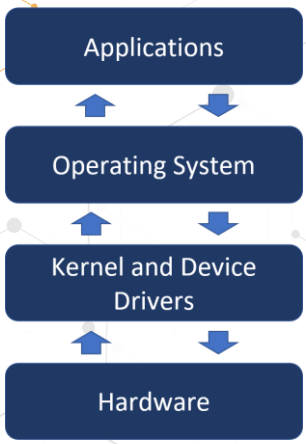
  

  - There are many evaluation models in use today.
    - The earliest one, which most security models are based on today is **"The Orange Book"** - The Trusted Computer System Evaluation Criteria – (TCSEC).
    - It was developed by the U.S. Department of Defense in the 1980s.
  - The Orange book was part of a Rainbow Series (or Rainbow Books).
    - The series also had a "The Red Book" Trusted Network Interpretation - (TNI). It addresses Network systems, whereas "The Orange Book" does not address Network Systems.

- **ITSEC** (The European Information Technology Security Evaluation Criteria):
  - Was the first successful international model. Contains a lot of references from The Orange Book, but both are retired now.
- **The International Common Criteria** (ISO/IEC 15408):
  - Common Criteria evaluations are performed on computer security products and systems.
  - To be of practical use, the evaluation must verify the target's security features. This is done through the following:
    - **Target Of Evaluation (TOE)** – The product or system that is the subject of the evaluation.
    - **Protection Profile (PP)** – A document which identifies security requirements for a class of security devices. Products can comply with more than one PP. Customers looking for particular types of products can focus on those products certified against the PP that meet their requirements.
    - **Security Target (ST)** – The document that identifies the security properties of the target of evaluation. The ST may have one or more PPs.

- **The International Common Criteria** (ISO/IEC 15408):
  - **Evaluation Assurance Level (EAL)** – How did the system or product score on the testing?
    - EAL Level 1-7:
      - → EAL1: Functionally Tested.
      - → EAL2: Structurally Tested.
      - → EAL3: Methodically Tested and Checked.
      - → EAL4: Methodically Designed, Tested and Reviewed
      - → EAL5: Semi-formally Designed and Tested.
      - → EAL6: Semi-formally Verified Design and Tested.
      - → EAL7: Formally Verified Design and Tested.

- **Secure System Design Concepts**
  - **Layering:** Separates hardware and software functionality into layers.
    - Layers can influence layers next to themselves, but not past that.
    - The change of a hard disk or memory to another of the same type or to a different type, has no influence on the applications.
    - The hard disk change may change the drivers in the "Kernel and device driver" level, but nothing past that.
    - The change of an OS (Operating System) may change which applications work or how the device drivers work, but it will not affect the hardware.



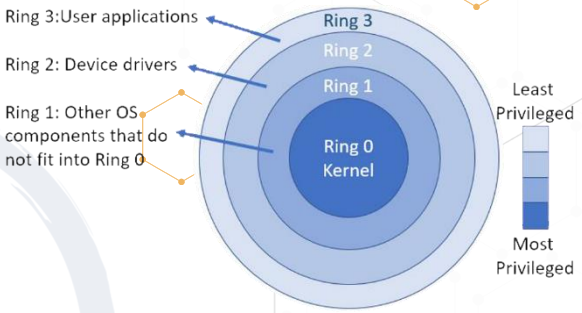
Not to be confused with the OSI model, this model is not as standardized, but you need to understand the concepts.

  - **Abstraction**: Hiding unnecessary details from the user, it provides a seamless experience for the user; they don't see the millions of background calculations.
  - **Security Domains:** A list of Objects a Subject is allowed to access, groups of Objects and Subjects with similar security requirements.
    - **Kernel mode** (Supervisor mode) is where the kernel lives, allowing low-level unrestricted access to memory, CPU, disk, etc. This is the most trusted and powerful part of the system. Crashes are not recoverable.
    - **User mode** (Problem mode) has no direct access to hardware, it is directed through an API (Application programming interface). Crashes are recoverable. This is most of what happens on a PC.
    - **Open and closed systems**:
      - **Open systems** use open standards and can use standard components from multiple vendors.

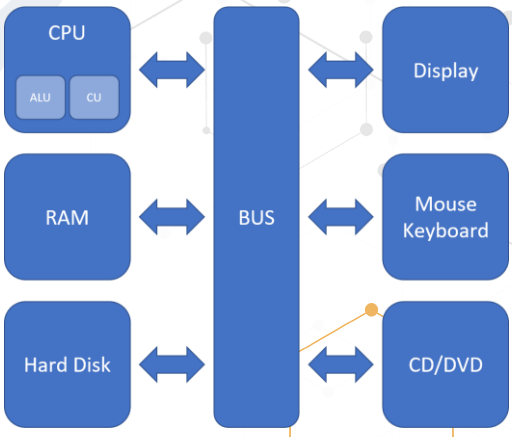
- → Hard disks are built and evaluated to a certain standard.
- → This is what most organizations use and is considered more secure.

- **Closed Systems** use proprietary hardware and software. This is "security through obscurity."
  - → You may not get hit with the latest Windows Server 2016 vulnerability, but your systems and software have not been as rigorously tested and audited for flaws as open systems and may be easy to gain access to.

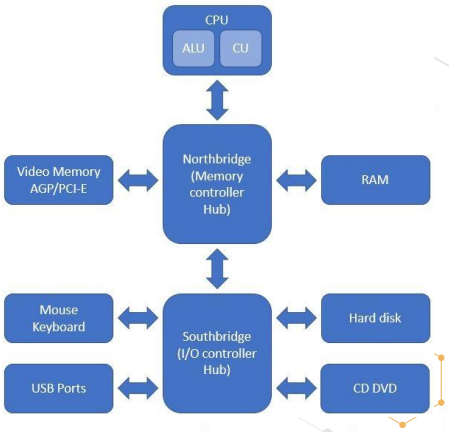
- **Security Domains:**
  - **The Ring Model**:
    - 4 ring model that separates Users (Untrusted) from the Kernel (Trusted).
    - The full model is slow and rarely used; most OSs only use rings 0 and 3.
    - There is a new addition to the Ring Model:
      - → Hypervisor mode is called Ring -1 and is for VM Hosts. Ring -1 sits below the Client kernel in Ring 0.



- **Secure Hardware Architecture:**
  - **System unit –** The case and all internal hardware.
  - **Motherboard** - Motherboard and CPU, memory slots, firmware, PCI slots.
  - **Peripherals** - Mouse, keyboard, monitors, anything plugged into the system unit.
  - **Regular computer bus** – The primary communications channel on a computer.
    - Communicates between internal hardware and I/O devices (Input/Output), keyboards, mice, monitors, webcams, etc.

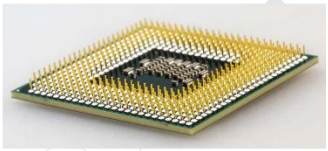


- **Northbridge and Southbridge**
  - This design is more common on newer computers and replaces the regular computer bus.
  - The Northbridge (Host bridge) is much faster than the Southbridge.
  - There are no North/Southbridge standards, but they must be able to work with each other.
  - There is a move towards integrating the Northbridge onto the CPU itself (Intel Sandy Bridge / AMD Fusion).

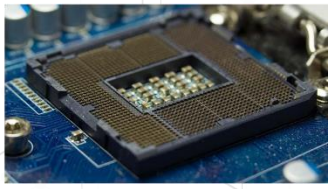


- **CPU (Central Processing Unit)**
  - **CPU (Central Processing Unit)** is the brains of the system.
    - It performs millions of calculations; everything a computer does is math.
    - CPUs are rated on their clock cycles per minute. Example: a 4.2GHz processor has 4.2 billion clock cycles per second.

CPU with Pins



CPU Socket



  - **Arithmetic logic unit (ALU)** performs arithmetic and logic operations.

    - It's a processor that registers the supply operands (Object of a mathematical operation) to the ALU and stores the results of ALU operations.
      It does all the math.
  - **Control unit (CU)** handles fetching (from memory) and execution of instructions by directing the coordinated operations of the ALU, registers and other components. It also sends instructions to the ALU.
    - **Fetch, Decode, Execute, and Store**
      - → **Fetch** - Gets the instructions from memory into the processor.
      - → **Decode** - Internally decodes what it is instructed to do.
      - → **Execute** - Takes the add or subtract values from the registers.
      - → **Store** - Stores the result back into another register (retiring the instruction).

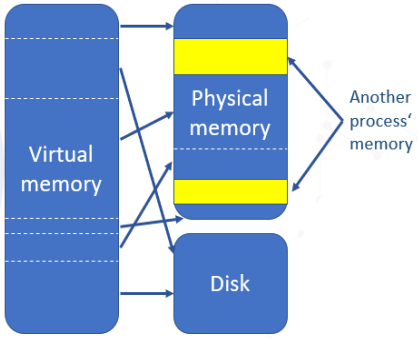
- **Pipelining** – Combining multiple steps into one process; can Fetch, Decode, Execute, Store in same clock cycle.

Instr. #	Pipeline Stage						
1	Fetch	Decode	Execute	Write			
2		Fetch	Decode	Execute	Write		
3			Fetch	Decode	Execute	Write	
4				Fetch	Decode	Execute	Write
5					Fetch	Decode	Execute
Clock Cycle	1	2	3	4	5	6	7

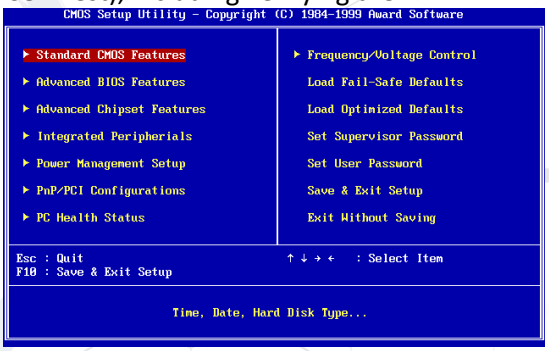
- Cycle 1. Fetch 1
- Cycle 2. Fetch 2, Decode 1
- Cycle 3. Fetch 3, Decode 2, Execute 1
- Cycle 4. Fetch 4, Decode 3, Execute 2, Write 1
- Cycle 5. Fetch 5, Decode 4, Execute 3, Write 2,
- Cycle 6. Decode 5, Execute 4, Write 3
- Cycle 7. Execute 5, Write 4

- **Interrupt:**
  - An interrupt is a signal to the processor emitted by hardware or software indicating an event that needs immediate attention.
  - An interrupt alerts the processor to a high-priority condition requiring the interruption of the current code the processor is executing.
  - When the higher priority task is complete the lower priority tasks will continue/be completed.
- **Processes and Threads:**
  - **Process**:
    - An executable program and its associated data loaded and running in memory.
    - A heavy weight process (HWP) is also called a task.
    - A parent process may spawn additional child processes called threads.
  - **Thread** – Light Weight Process (LWP).
    - Threads can share memory, resulting in lower overhead compared to heavy weight processes.
    - Processes may exist in multiple states:
      - New: a process being created.
      - Ready: a process waiting to be executed by the CPU.
      - Running: a process being executed by the CPU.
      - Blocked: waiting for I/O.
      - Terminate: a completed process.
- **Multithreading, Processing, Tasking, and Programming.**
  - **Multithreading** is the ability of a central processing unit (CPU) or a single core in a multi-core processor to execute multiple processes or threads concurrently, appropriately supported by the operating system.
  - **Multiprocessing** - A computer using more than one CPU at a time for a task.
  - **Multitasking** - Tasks sharing a common resource (1 CPU).
  - **Multiprogramming** - A computer running more than one program at a time (Word and Chrome at the same time).

- **Memory protection** prevents one process from affecting the confidentiality, integrity, or availability of another. Used to protect user/process data in multi-user and multitasking environments.
- **Process isolation** is a logical control that tries to prevent one process from Interfering with another.
- **Hardware segmentation** takes that a step further by mapping processes to specific memory locations.
- **Virtual Memory** provides virtual address mapping between applications and hardware memory. Virtual memory is used for many things: multitasking, multiprocessing, swapping, to name a few.



- **Swapping** moves entire processes from primary memory (RAM) from/to secondary memory (Disk).
- **Paging** copies a block from primary memory (RAM) from/to secondary memory (Disk).
- **BIOS –** Basic Input Output System (Low level OS):
  - The BIOS runs a basic POST (Power On Self Test), including verifying the integrity of the BIOS, testing the memory, identifying system devices, and more.
  - Once the POST process is complete and successful, it locates the boot sector for the OS.
  - The kernel loads and executes, and the OS boots.
  - BIOS is stored on ROM - most likely EEPROM now (or EPROM on older systems).



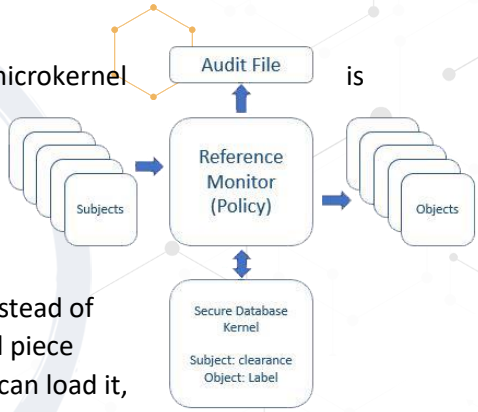
- **WORM Media** (Write Once Read Many):
  - ROM is a WORM Media (not in use, though).
  - CD/DVDs can be WORM Media (R) if they are not R/W (Read/Write).

- **TPM** (Trusted Platform Module):
  - Is an international standard for a secure cryptoprocessor which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.
  - TPM can be used for RNG (Random Number Generation), Symmetric Encryption, Asymmetric Encryption, Hashing Algorithms, and secure storage of cryptographic keys and message digests.
  - It is most commonly used to ensure boot integrity.

- **Data Execution Prevention** (DEP) is a security feature that can prevent damage to your computer from viruses and other security threats.

- Harmful programs can try to attack Windows by attempting to execute code from system memory locations reserved for Windows and other authorized programs; DEP prevents that.
- **Address Space Layout Randomization** (ASLR) is a memory-protection process for OS's; it guards against buffer-overflow attacks by randomizing the location where system executables are loaded into memory.

- **Secure OS and Software Architecture**
  - **The Kernel**
    - At the core of the OS is the Kernel. At ring 0 (or 3), it interfaces between the operating system (and applications) and the hardware.
    - A **monolithic kernel** is one static executable and the kernel runs in supervisor mode. All functionality required by a monolithic kernel must be precompiled in.
    - **Microkernels** are modular kernels. A microkernel is smaller and has less native functionality than a monolithic kernel. They can add functionality via loadable kernel modules. Microkernels may also run kernel modules in user mode ring 3, instead of supervisor mode. If a non-precompiled piece of hardware is added the Microkernel can load it, making the hardware work.



    - The **reference monitor** is a core function of the kernel; it handles all access between subjects and objects. It is always on and can't be bypassed.

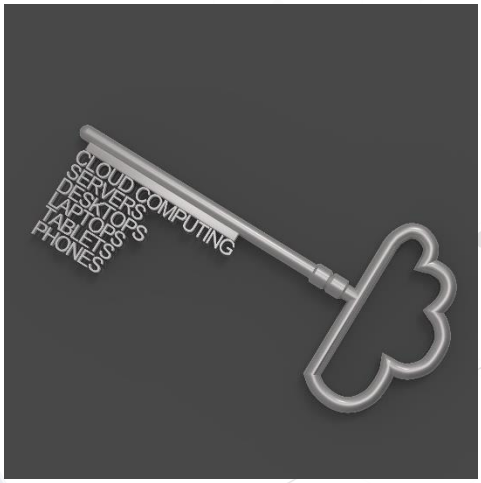
- **Users and File Permissions**
  - **Linux/UNIX**
    - Read (r), Write (w) and Execute (x) permissions which can be set at an owner, group or world level.
  - **Windows NTFS** (New Technology File System)
    - Read, Write, Read and Execute, Modify, Full Control (Read, Write, Execute, Modify, Change Permissions).
    - It is a type of DAC (Discretionary Access Control) – Who can access and how they can access it is at the owner's discretion.

Virtualization and Distributed Computing

- **Virtualization**

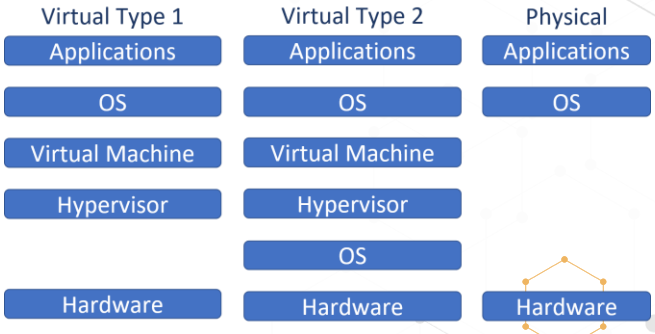
Virtualization poses a new whole set of standards, best practices and security concerns.

- With Virtualization, we have many servers (clients) on the same hardware platform (host).
- Virtualization is software running under the OS and above the Hardware (Ring -1).
- Traffic between the clients on the host doesn't have to traverse our network.
- Common Virtualization software could be VMWare, Hyper-V, or Xen.
- With Distributed Computing we use either multiple local or remote clients for our needs, most commonly cloud computing. How do we ensure the cloud Data Center meets our security posture, how do they segment their network?



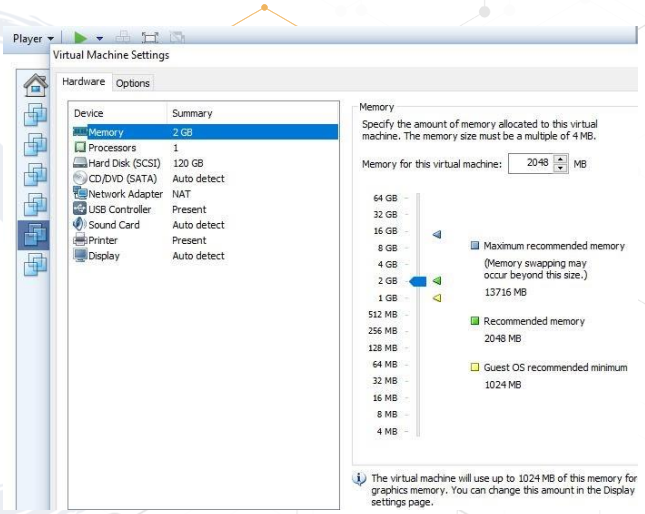
- **Virtualization holds a ton of benefits:**
  - Virtualized environments cost a lot less than all physical servers.
  - It is much easier to stand up new servers (don't need to buy hardware, wait 2 weeks, rack it, run power/internet).
  - You can easily back up servers with snapshots; server builds can be done with images.
  - You can instantly reallocate resources.
  - They have lower power and cooling costs, a much smaller rack footprint (50-100 servers in the space of 5-8).

- **Hypervisor** - Controls the access between the virtual guest/clients and the host hardware.



  - Type 1 hypervisor (Bare Metal) is a part of a Virtualization OS that runs on top of the host hardware (Think Data Center).
  - Type 2 hypervisor runs on top of a regular OS like Windows 10 - (Think your PC).

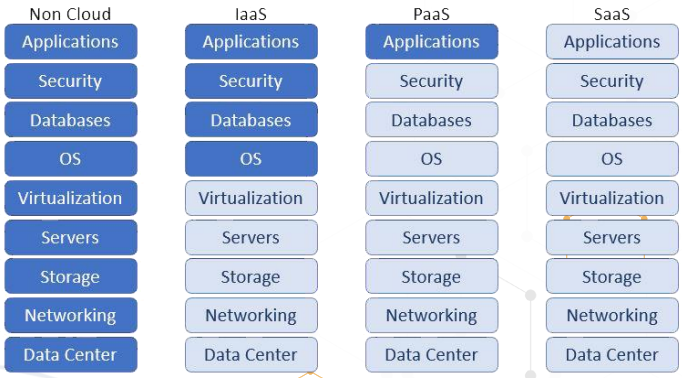
- **VM Escape** (Virtualization escape) is when an attacker can jump from the host or a client to another client, this can be even more of a concern if you have different Trust Level Clients on the same host. They should ideally be on separate hosts.



- **Hypervisor Security** - If an attacker can get access to the hypervisor, they may be able to gain access to the clients.
- **Resource Exhaustion** - Admins oversubscribe the CPU/Memory and do not realize more is needed (availability).

- **Cloud Computing**
  - **Cloud Computing** can be divided into 3 main types:
    - **Private Cloud Computing** - Organizations build and run their own cloud infrastructure (or they pay someone to do it for them).
    - **Public Cloud Computing** - Shared tenancy – A company builds massive infrastructures and rents it out to anyone who wants it. (Amazon AWS, Microsoft, Google, IBM).
    - **Hybrid Cloud Computing** – A mix of Private and Public Cloud Computing. An organization can choose to use Private Cloud for sensitive information and Public Cloud for non-sensitive data.
    - **Community Cloud Computing** – Only for use by a specific community of consumers from organizations that have shared concerns. (Mission, policy, security requirements, and/or compliance considerations.)

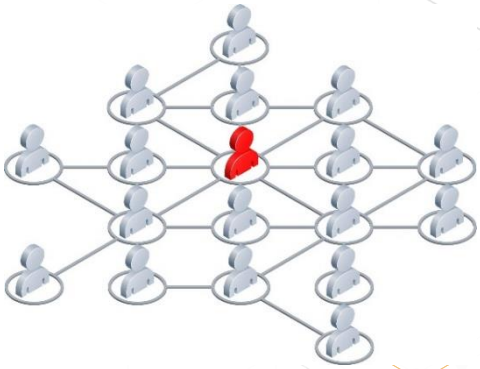
- Platforms are normally offered as:
  - **IaaS** - (Infrastructure as a Service) The vendor provides infrastructure up to the OS, the customer adds theOS and up.
  - **SaaS** - (Software as a Service) The vendor provides the OS and applications/programs. Either the customer interacts with the software manually by entering data on the SaaS page, or data is automatically pushed from your other applications to the SaaS application (Gmail, Office 365, Dropbox, Payroll).



  - **PaaS** - (Platform as a Service) The vendor provides pre-configured OSs, then the customer adds all programs and applications.

- **Grid Computing** – can make use of resources not currently in use from 100 or 100,000s of computers to perform very complex tasks.
  - Each node has a smaller subtask but leveraging the entire Grid can make it very powerful and fast.
  - Often used in problems so complex that they need that many nodes to be solved.
  - BOINC (Berkeley Open Infrastructure for Network Computing) has over 4,000,000 machines enrolled, used for a wide variety of scientific research.

- **Peer to Peer** (P2P) - Any system can be a client and/or a server.
  - Most commonly used on torrent networks to share music, movies, programs, pictures, and more (The majority without the copyright holder's consent).
  - Older versions had centralized index servers making it easier to disrupt a sharing network, but the current version uses no centralized infrastructure.



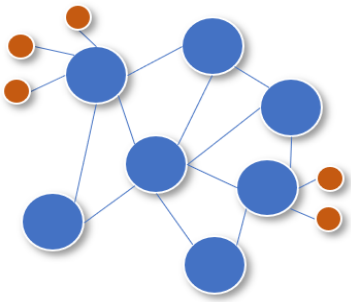
  - Each client is often also a server and has the index. Taking down 10,000 in a network of 100,000 will just result in a network of 90,000 with no other discernable impact.

- **Thin Clients** (Boot sequence - BIOS > POST > TCP/IP > BOOTP or DHCP)
  - **Diskless Workstation** (Diskless node) has all the normal hardware/firmware except the disk, and the low-level OS (BIOS), which performs the POST. It then downloads the kernel and higher-level OS.
  - **Thin Client Applications** - We use a Web Browser to connect to the application on a server on port 80 (HTTP) or port 443 (HTTPS). The full application is housed and executed on the server vs. on your PC.

Virtualization, Cloud, and Distributed Computing:

- **Thin Clients** (Boot sequence - BIOS > POST > TCP/IP > BOOTP or DHCP)
  - **Diskless Workstation** (Diskless node) has all the normal hardware/firmware except the disk, and the low-level OS (BIOS), which performs the POST. It then downloads the kernel and higher-level OS.
  - **Thin Client Applications** - We use a Web Browser to connect to the application on a server on port 80 (HTTP) or port 443 (HTTPS). The full application is housed and executed on the server vs. on your PC.
- **Distributed systems**
  - **Can also be referred to as:**
    - Distributed computing environment (DCE), concurrent computing, parallel computing, and distributed computing.
  - A collection of individual systems that work together to support a resource or provide a service.
  - Most end-users see the DCE as a single entity and not as multiple systems.

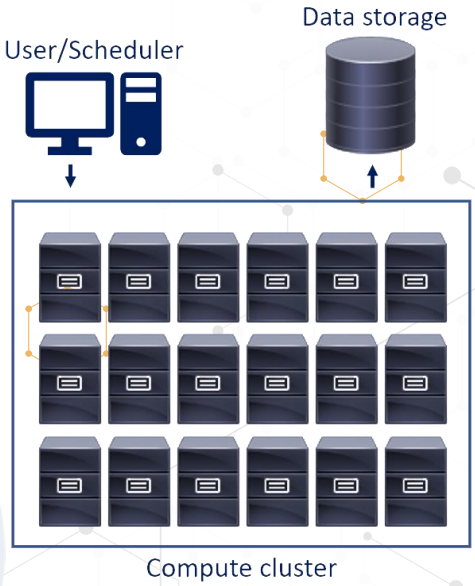
Centralized system



Distributed system

- **Why do we use DCEs?**
  - They can give us horizontal scaling (size, geography, and administration), modular growth, fault tolerance, cost-effectiveness, low latency (users connect to the closest node).
- **Where do we use DCEs?**
  - All over the place (The internet, websites, cell networks, research, P2P networks, blockchain, …).

- **High-Performance Computing (HPC) systems:**
  - Most often aggregates of compute nodes in a system designed to solve complex calculations or manipulate data at very high speeds.
  - HPCs have 3 components. Compute, network, and storage.
    - All 3 must have enough resources to not become a bottleneck.
  - Most well-known versions are super computers.



- **Edge computing systems:**
  - The processing of data is done as close as possible to where it is needed, we do that by moving the data and compute resources.
  - This will optimize bandwidth use and lower latency.
  - CDN's are one of the most common types of edge computing.
  - 80%+ of large enterprises have already implemented or are in the profess of implementing an edge computing strategy.

The Internet of Things (IoT)

- It is really anything "Smart": Smart TVs, Thermostats, Lightbulbs, Cars, anything that connects to the internet in some way (that didn't before).
- They can be an easy way into your smart device, as most are never patched (many don't even have the option).
- Most devices have very basic security (if any). They use the default login/password and they often use well-known ports, making them easy to target. We harden here, we patch, segment the network, lock ports, and change defaults.

- They are not only simple to hack but can also provide attackers an easy way onto your network. If you use it in your organization or at home, segment that part of the network off from everything else and lock it down.

Emanations and Covert Channels

- **Emanations** - Often Electromagnetic Emanations.
  - Information that can be disseminated from the electrical changes from a system or a wire.
  - It is possible to log a user's keystrokes on a smart phone using the motion sensor.
  - It is unintentional information-bearing signals, which - if intercepted and analyzed - can lead to a compromise.
  - We can protect against Electromagnetic Emanations with heavy metals, but we would have 80 lbs. (40 kgs.) laptops.
- **Covert Channels** – Creates the capability to transfer information using channels not intended to do so.
  - **Covert Timing Channels:** Operations that affect the "real response time observed" by the receiver.
    - Most common is username/password - wrong username takes 100ms to confirm, wrong password takes 600ms to confirm, you get the "Wrong username or password" error, but an attacker can tell when they use a correct username because of the delay difference.
  - **Covert Storage Channels:** Hidden information through the modification of a stored object.
    - Certain file sizes have a certain meaning.
    - Attackers can add data in payload if outbound ICMP packets (Unless we need it, block outbound ICMP packets).
  - **Steganography** - Hiding a message within another media (invisible ink and the hidden clues in da Vinci's paintings).
    - The messages can be hidden in anything really, most commonly images and soundtracks.
    - On images like this one, the program changes the shading of some of the pixels of the image. To the naked eye, it is not noticeable, but a lot of information can be hidden in the images this way.
    - Hidden in the bottom image is the first chapter of *Great Expectations* (Charles Dickens, 1867 Edition - 4 pages at font size 11, 1827 words, 7731 characters).

Original image

Altered image

  - **Digital Watermarks** encode data into a file.
    - The watermark may be hidden, using steganography, or visible watermarks.
    - Often used to fingerprint files (the file is identified as yours).

System Vulnerabilities, Threats, and Countermeasures

- **Malware**
  - **Malware (Malicious Code) -** This is the catch-all name for any malicious software used to compromise systems or data.
    - **Viruses** - require some sort of human interaction and are often transmitted by USB sticks or other portable devices.
      When the program is executed, it replicates itself by inserting its own code into other programs.
      - **Macro** (document) Viruses: Written in Macro Languages, embedded in other documents (Word, Outlook).
      - **Boot Sector** Viruses: Infect the boot sector or the Master Boot Record, ensuring they run every time the PC boots.
      - **Stealth** Viruses: Try to hide themselves from the OS and antivirus software.
      - **Polymorphic** Viruses: Change their signature to avoid the antivirus signature definitions.
      - **Multipart** (Multipartite) Viruses**:** Spread across multiple vectors. They are often hard to get rid of because even if you clean the file infections, the virus may still be in the boot sector and vice-versa.

    - **Worms** - spread through self-propagation - they need no human interaction; they do both the payload damage and replicate through aggressive network use (also makes them easier to spot).
    - **Trojans** - malicious code embedded in a program that is normal. This can be games, attachments, website clicks, etc. …
    - **Rootkits** - Replace some of the OS/Kernel with a malicious payload. User rootkits work on Ring 3 and Kernel rootkits on Ring 0.
    - **Logic Bombs -** Malicious code that executes at a certain time or event - they are dormant until the event (IF/THEN).
      - IF Bob is not getting an annual bonus over $10,000, THEN execute malicious code.
      - IF date and time is 5/15/18 00:02:12, THEN execute malicious code.

- **Packers** – Programs to compress *.exe files, which can be used to hide malware in an executable, neutral technology.
- **Antivirus Software** - tries to protect us against malware.
    - **Signature** based - looks for known malware signatures - MUST be updated constantly.
    - **Heuristic** (Behavioral) based - looks for abnormal behavior - can result in a lot of false positives.

- **Server (Service) Side Attacks:**
    - Attacks directly from an attacker to a target.
    - Defense in Depth can mitigate some of these.
    - The term "Server" does not mean only servers, just that the attack is directly aimed at the end target. (They come to you).
- **Client-Side Attacks:**
    - The client initiates, then gets infected with malicious content usually from web browsers or instant messaging applications. (You go to them).
    - Since most firewalls protect inbound mostly, client-side attacks are often more successful.

- **Web Architecture and Attacks**
    - **Applets:** Small applications often embedded into other software (web browsers).
        - They are executable, downloaded from a server and installed locally on the client.
        - Applets are commonly written in Java or ActiveX (control).
            - **Java** applets run in a sandbox environment - segmenting the java from the OS (limiting some threats), OS agnostic.
            - **ActiveX** runs with certificates (not sandbox) - since ActiveX is an MS product it interacts more with the OS (Windows only).

    - **OWASP** (Open Web Application Security Project) 2017 - has a Top 10 of the most common web security issues.
        - A1: Injection
        - A2: Broken Authentication
        - A3: Sensitive Data Exposure
        - A4: XML External Entities (XXE)
        - A5: Broken Access Control
        - A6: Security Misconfiguration
        - A7: Cross-Site Scripting (XSS)

- A8: Insecure Deserialization
- A9: Using Components with Known Vulnerabilities
- A10: Insufficient Logging & Monitoring

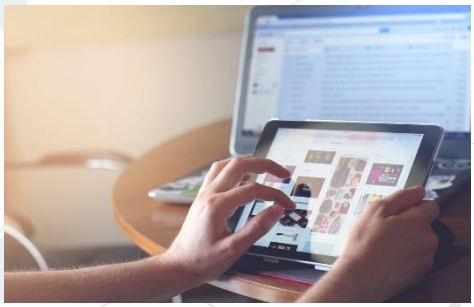
- **XML** (Extensible Markup Language) is a markup language designed as a standard way to encode documents and data.
  - It is similar to HTML, but more universal.
  - It is mainly used for Web but does not have to be, it can be used to store application configuration, output from auditing tools, and many other things.

- **SOA** (Service-Oriented Architecture) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network.
  - The basic principles of service-oriented architecture are independent of vendors, products, and technologies.
  - SOA is intended to allow multiple different applications to be consumers of services.

- **Database Security**
  - **Polyinstantiation** (Alternative Facts) – Two (or more) instances of the same file depending on who accesses it.
    - The real information may be available to subjects with Top Secret clearance, but different information will be available to staff with Secret or lower clearance.
  - **Aggregation** is a collection or gathering of data together for the purpose of statistical analysis. (You see the bigger picture rather than the individual pieces of data).
  - **Inference** requires deducing from evidence and reasoning rather than from explicit statements.
  - **Data mining** is the computing process of discovering patterns in large data sets.
    - It uses methods combining machine learning, statistics, and database systems.
  - **Data Analytics** is looking at what normal operations look like, then allowing us to identify abuse more proactively from insider threats or compromised accounts.
    - We mitigate the attacks with **Defense in Depth** (again) – We secure the building, the entrances, the doors, the network, the servers, the OS, the DB, screen the employees, … We have solid policies, procedures, standards, and guidelines.

- **Mobile Security:**
  - **Cell phones** are the mobile devices most often lost – Current Android and iOS phones all have full disk encryption.
    - We can add a lot more features to our company cell phones to make them more secure.
    - Remote wipe, find my device, lock after x minutes, number of failed passwords, disable removable storage, …
    - We can also use a centralized management system: **MDM** (Mobile Device Management) controls a lot of settings.
      - App Black/White list, Storage Segmentation, Remote Access Revocation, Configuration Pushes, Backups.
      - More controversial: Track the location of employees, monitor their data traffic and calls.

  - Laptops, Smartphones and Tablets are great productivity tools, but they (just like anything else) have to be secured properly or they are a liability.
    - BYOD (Bring Your Own Device) - There should be clear corporate policies/procedures/guidelines.
    - On/off boarding - How is the return of mobile devices handled and enforced?
    - It is much harder to standardize on BYOD. Is support staff ready for that many devices, OSs, applications?
    - Should we use MDM?
    - How do we handle patch and virus management?

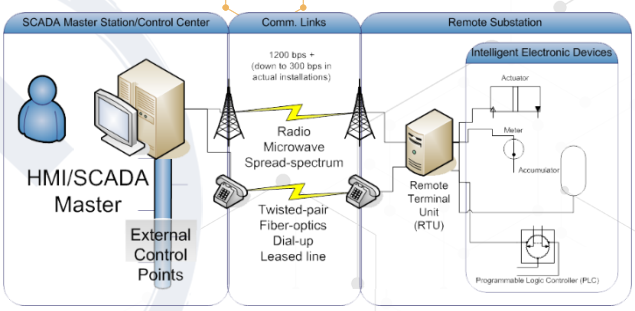


- **Industrial Control System**
  - **ICS** – (Industrial Control System) is a general term for several types of control systems and associated instrumentation used in industrial production technology.
    - **SCADA** (Supervisory Control And Data Acquisition) is a control system architecture that uses computers, networked data communications and graphical user interface (GUI) for high-level process supervisory management.
      - The operator interfaces which enable monitoring and the issuing of process commands, such as controller set point changes, are handled through the SCADA supervisory computer system.

- However, the real-time control logic or controller calculations are performed by networked modules which connect to the field sensors and actuators.

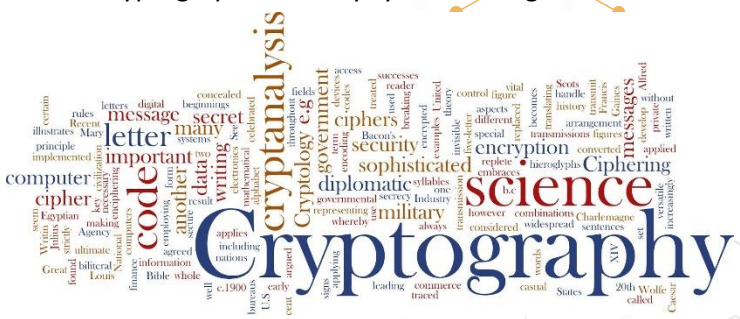
- **DCS** (Distributed Control Systems) is a computerized control system for a process or plant in which autonomous controllers are distributed throughout the system, but there is central operator supervisory control.
- **PLC** (Programmable Logic Controllers) is an industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes such as assembly lines, robotic devices or any activity that requires high reliability control, ease of programming and process fault diagnosis.

- **DNP3** (Distributed Network Protocol)
  - A set of communications protocols used between components in process automation systems.
  - Mainly used in utilities such as electric and water companies.
  - It plays a crucial role in SCADA systems, where it is used by SCADA Master Stations (Control Centers), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs).
  - It is primarily used for communications between a master station and RTUs or IEDs.



Cryptography – The Science of Secure Communication

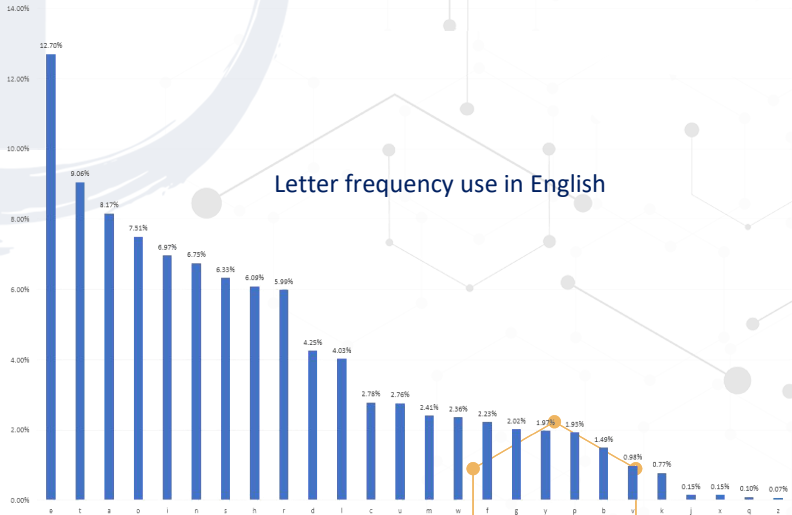
- **Definitions:**
  - **Cryptology** is the science of securing communications.
  - **Cryptography** creates messages where the meaning is hidden.
  - **Cryptanalysis** is the science of breaking encrypted communication.
    - Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.



- It uses mathematical analysis of the cryptographic algorithm, as well as side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation and the devices that run them.

- **Cipher** is a cryptographic algorithm.
  - **Plaintext** (Cleartext) is an unencrypted message.
  - **Ciphertext** is an encrypted message.
  - **Encryption** converts the plaintext to a ciphertext.
  - **Decryption** turns a ciphertext back into a plaintext.
- **Book Cipher** - Use of a well-known text (Often a book) as the key.
  - Messages would then look like 244.2.13, 12.3.7, 41.42.1. ...
  - The person reviewing the message would look at page 244, sentence 2, word 13, then page 12, sentence 3, word 7, page 41, sentence 42 word 1, ...
- **Running-Key Cipher** – uses a well-known test as a key as well but uses a previously agreed upon phrase.
  - If we use the CISSP Code of Ethics preamble "The safety and welfare of society and the common good..."
  - The sender would add the plaintext message to the letters from the key, and the receiver would subtract the letters from the key.

- **Mono and Polyalphabetic Ciphers:**
  - **Monoalphabetic Ciphers** - Substitutes one letter for another - "T" would be "W" for instance - very easy to break with frequency analysis (or even without).
  - **Polyalphabetic Ciphers** - Similar but uses different starting points each round, "T" may be "W" on first round, but "D" on second round, more secure, but still not very secure.
  - **Frequency Analysis** (analyzing the frequency of a certain character) – In English “E” is used 12.7% of the time. Given enough encrypted substitution text, you can break it just with that.



Letter frequency use in English

- **Exclusive Or (XOR)**

  XOR is very useful in basic cryptography; we add a key to the plaintext to make the ciphertext. If we have the Key, we can decipher the Cipher text. Used in most symmetric encryption (or at least used in the algorithm behind it).

  - **Confusion** is the relationship between the plaintext and ciphertext; it should be as random (confusing) as possible.
  - **Diffusion** is how the order of the plaintext should be "diffused" (dispersed) in the ciphertext.
  - **Substitution** replaces one character for another, this provides diffusion.
  - **Permutation** (transposition) provides confusion by rearranging the characters of the plaintext.

XOR truth table

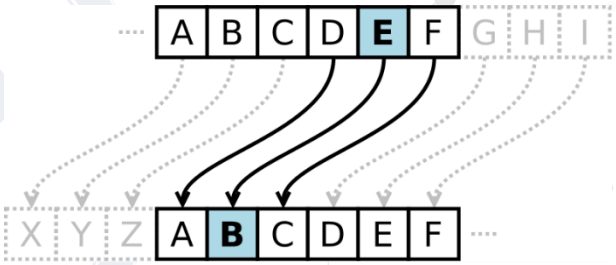
Input		Output
A	B	
0	0	0
0	1	1
1	0	1
1	1	0

0 = false, 1 = true

Plain text 0010101010
Key 1010011001
Ciphertext 1000110011

- **The History of Cryptography** (yes, this is testable).

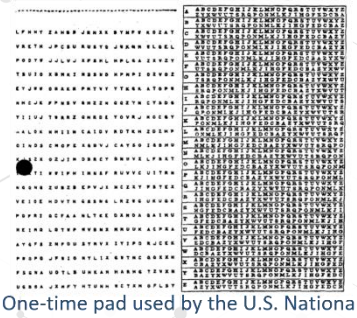
  - **Spartan Scytale** - Message written lengthwise on a long thin piece of parchment wrapped around a certain size round stick. By itself it would make no sense, but if rewrapped around a stick of the same diameter it would be decipherable.



  - **Caesar Cipher** (Substitution) - Done by switching Letters by a certain number of spots in the alphabet. "Pass the exam" moved 3 back would be "Mxpp qeb buxj."

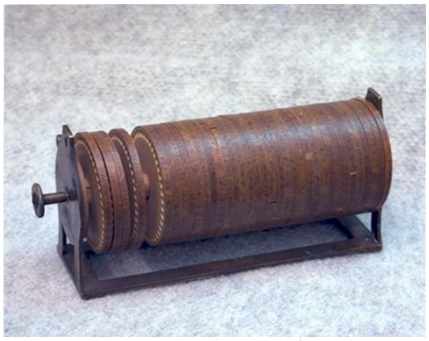
  - The **Vigenère cipher** is a polyalphabetic cipher named after Blaise de Vigenère, a French cryptographer who lived in the 16th century.
    - The alphabet is repeated 26 times to form a matrix (Vigenère Square).
    - It uses the plaintext (x axis) and a key (y axis).
      - If the plaintext is CISSP and the key is THOR, the ciphertext would be VPGJI.
      - The key wraps if the plaintext is longer than the key (it normally is).

- **Cipher Disk** - 2 concentric disks with alphabets on them, either just as agreed upon "T" is "D" (monoalphabetic) or "T" is "D" again, but the inner disk is turned in a pre-agreed upon direction and turns every X number of letters (decoder rings).
- **Enigma** - Rotary based. Used 3 rotors early on, which was broken, so the Germans added 1 rotor, making it much harder. Breaking the Enigma was responsible for ending the war early and saving millions of lives.
- **Purple** (US name) - Japanese rotary based, very similar to the Enigma.
  - Broken by the US, England, and Russia (3 rotors).
  - When the Russians learned Japan was not attacking them, they moved the majority of their eastern troops to Moscow to fight the Germans. They had decoded that Japan was going for Southeast Asia.
- **One-Time Pad:**
  - Cryptographic algorithm where plaintext is combined with a random key.
  - It is the only existing mathematically unbreakable encryption.
    - While it is unbreakable it is also very impractical.
    - It has ONE use per pad; they should never be reused.
    - Characters on the pad have to be truly random.
    - The pads are kept secure.
- **Vernam Cipher** (The first known use of a one-time pad).
  - It used bits, and the bits were XORed to the plaintext bits.
- Project **VENONA** was a project by the US and the UK to break the KGB's encryption from 1943 to 1980.
  - The KGB used one-time pads (unbreakable if not reused) for sensitive transmissions.
  - The KGB reused pads, many messages were decoded, leading to the arrest of many high-profile US residents.

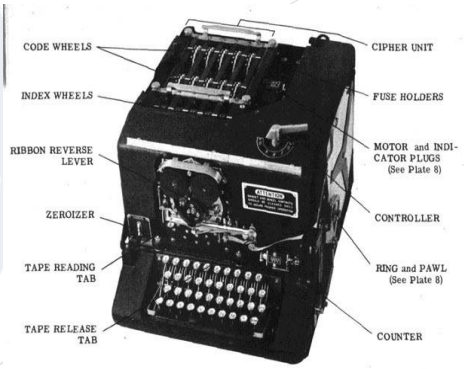


One-time pad used by the U.S. National Security Agency, code named DIANA

- **The Jefferson Disk** (Bazeries Cylinder) - is a cipher system using a set of wheels or disks, each with the 26 letters of the alphabet arranged around the edge. Jefferson (US president) invented it, and Bazeries improved it.
  - The order of the letters is different for each disk and is usually scrambled in some random way.
  - Each disk is marked with a unique number.
  - A hole in the center of the disks allows them to be stacked on an axle.
  - The disks are removable and can be mounted on the axle in any order desired.
  - The order of the disks is the cipher key, and both sender and receiver must arrange the disks in the same predefined order.
  - Jefferson's device had 36 disks.



- **SIGABA:**
  - A rotor machine used by the United States throughout World War II and into the 1950s, similar to the Enigma.
  - It was more complex, and was built after examining the weaknesses of the Enigma.
  - No successful cryptanalysis of the machine during its service lifetime is publicly known.
  - It used 3x5 sets of rotors.
  - The SIGABA was very large, heavy, expensive, difficult to operate, mechanically complex, and fragile.



- *With the common use of Cryptography, many governments realized how important it was that cryptographic algorithms were added to export restrictions in the same category as munitions.*
  - **COCOM** (Coordinating Committee of Multilateral Export Controls) 1947 – 1994.
    - Was used to prevent the export of "Critical Technologies" from “Western” countries to the "Iron Curtain" countries during the cold war.
    - Encryption is considered "Critical Technologies"
  - **Wassenaar Arrangement -** 1996 – present.
    - Similar to COCOM, but with former "Iron Curtain" countries being members
    - Limits exports on military and "dual-use” technologies. Cryptography is part of that.

- Some nations also use it to prevent their citizens from having strong encryption (easier to spy on your own people if they can't use strong cryptography).

- **Asymmetric vs Symmetric Encryption and Hybrid**
  - **Asymmetric**
    - Pros: It does not need a pre-shared key, only 2x users = total keys.
    - Cons: It is much slower; it is weaker per bit.
  - **Symmetric**:
    - Pros: Much faster, stronger per bit.
    - Cons: Needs a pre-shared key, **n(n-1)/2** users, becomes unmanageable with many users.
  - **Hybrid Encryption:**
    - Uses Asymmetric encryption to share a Symmetric Key (session key).
    - We use the security over an unsecure media from Asymmetric for the initial exchange and we use the speed and higher security of the Symmetric for the actual data transfer.
    - The Asymmetric Encryption may send a new session key every so often to ensure security.

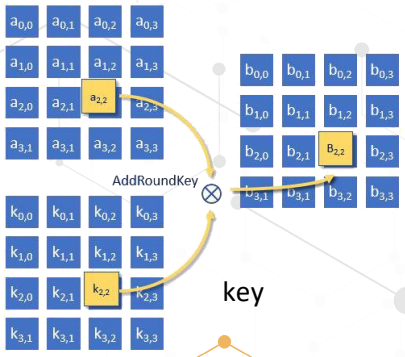
Users	Symmetric keys	Asymmetric Keys
2	1	4
5	10	10
10	45	20
30	435	60
100	4,950	200
500	124,750	1000
5000	12,497,500	10000
10000	49,995,000	20000

- **Symmetric Encryption:**
  - **DES** - Data Encryption Standard (Single DES).
    - For the exam it may be called DEA (algorithm) or DES (standard)
    - No longer secure and it has multiple attack vectors published.
    - Symmetric – 64-bit block cipher – 56-bit key, 16 rounds of encryption, uses Feistel.

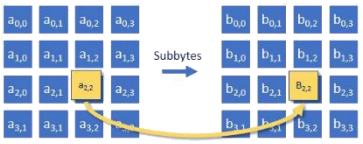
    DES has 5 different modes it can encrypt data with, they include: Block, Stream, Initialization Vector and if encryption errors propagate to the next block.
    - **ECB** (Electronic Code Book) - The simplest and weakest, no initialization vector or chaining.
      - 2 separate encryptions with same plaintext would produce identical ciphertext.
    - **CBC** (Cipher Block Chaining) - Uses initialization vectors and chaining.
      - The first block uses an initial Vector and every subsequent block uses XOR from the first block
      - The weakness is an encryption error which will propagate through all blocks after the error since they build on each other, breaking integrity.
    - **CFB** (Cipher Feedback) Very similar to CBC, but uses stream cipher, not block.
      - It uses feedback (chaining in a stream cipher), initialization vector and it has the same error propagation.

- **OFB** (Output Feedback) Similar to CFB, but instead of the previous ciphertext for the XOR it uses the subkey before it is XORed to the plaintext.
  - Doing it this way makes the encryption errors NOT propagate.
- **CTR** (Counter) - Similar to OFB, but it uses the Feedback differently, the way it uses the Feedback can be simple as ascending numbers.
  - First block XORed with 1, second block with 2, third block with 3, since the Feedback is predictable it can be done in parallel.

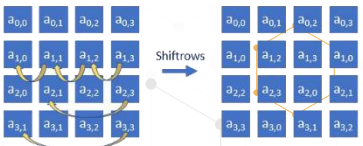
- **3 DES** (Triple DES):
  - Was developed to extend life of DES systems while getting ready for AES.
  - Symmetric – 64-bit block cipher – 56-bit key, 16 rounds of encryption, uses Feistel.
  - 3 rounds of DES vs 1.
    - K1 (keymode1) - 3 different keys with 112-bit key strength.
    - K2 (keymode2) - 2 different keys with 80-bits and 1/3 same key.
    - K3 (keymode3) – Same key 3 times, just as insecure as DES (encrypt/decrypt/encrypt).
  - Considered secure until 2030 and still commonly used (K1).
- **IDEA** (International Data Encryption Algorithm):
  - Designed to replace DES.
  - Symmetric, 128-bit key, 64-bit block size, considered safe.
  - Not widely used now since it is patented and slower than AES.
- **AES** - Advanced Encryption Standard (Rijndael).
  - Symmetric.
  - Considered secure.
  - Open source.
  - Uses both transposition and substitution.
  - Widely used today.
  - AES operates on a 4 × 4 column-major order matrix of bytes.
  - **Initial Round**:
    - **AddRoundKey** — each byte is combined with a block of the round using bitwise XOR.



- **Rounds**:
  - **SubBytes** — a non-linear substitution step where each byte is replaced with another according to a lookup table.
  - **ShiftRows** — a transposition step where the last three rows of the state are shifted a certain number of steps.
  - **MixColumns** — a mixing operation which operates on the columns, combining the four bytes in each column.

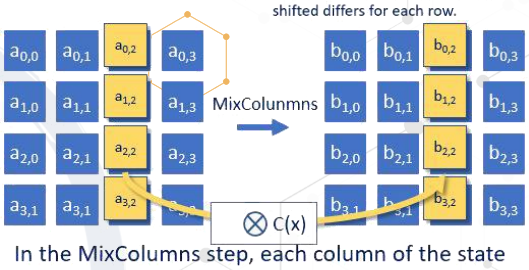


In the SubBytes step, each is replaced with its entry in a fixed 8-bit lookup table



In the ShiftRows step, bytes in each row are shifted to the left. The number of places each byte is shifted differs for each row.

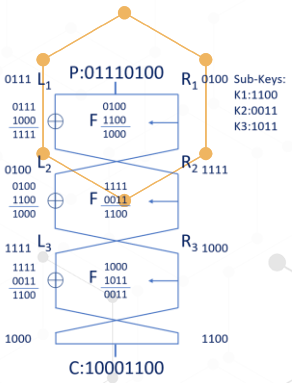
- **Final Round** (no MixColumns):
  - SubBytes
  - ShiftRows
  - AddRoundKey
- The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the plaintext into the ciphertext.
- The number of cycles depends on the key length:
  - 10 cycles for 128-bit keys.
  - 12 cycles for 192-bit keys.
  - 14 cycles for 256-bit keys.



In the MixColumns step, each column of the state is multiplied with a fixed polynomial *c(x)*

- **Blowfish** - publish domain.
  - Uses Feistel.
  - Symmetric, block cipher, 64-bit blocks, 32 – 448-bit key lengths.
  - No longer considered secure.
  - Developer recommends using Twofish.
- **Twofish**
  - Uses Feistel.
  - Symmetric, block cipher 128-bit blocks, key length 128, 192, 256 bits.
  - Considered secure.

- **Feistel cipher (Feistel network)**
  - The Cipher splits a plaintext block into two halves (L and R).
  - The process goes through several rounds, the right half of the block does not change.
  - The right half (R_n) is XORed with a subkey (K_n) for each round (F).
  - The XORed value (F) is XORed with the left block (L_n).



- The recipient reverses the subkey order and XORs to get the plaintext.
- **Feistel or modified Feistel Algorithms:**
  - Blowfish, Camellia, CAST-128, DES, FEAL, ICE, KASUMI, LOKI97, Lucifer, MARS, MAGENTA, MISTY1, RC5, TEA, Triple DES, Twofish, XTEA, …
- **Generalized Feistel Algorithms:**
  - CAST-256, MacGuffin, RC2, RC6, Skipjack.

- **RC4:**
  - Used by WEP/WPA/SSL/TLS.
  - Pseudorandom keystream.
  - No longer considered secure.
  - Symmetric, Stream cipher, 40 – 2048-bit key length.
- **RC5:**
  - Symmetric, Block Cipher, 32, 64, and 128-bit blocks, Key length 0 – 2040-bits, uses Feistel.
  - Considered Secure (if high enough blocks/key).
- **RC6** – AES3 Finalist:
  - Based on RC5, but changed to meet AES requirements, uses Feistel.
  - Symmetric, Block Cipher, 128-bit blocks, 128, 192, and 256-bit key length.
  - Considered Secure.

- **Asymmetric Encryption** (Public Key Encryption)

  We have used symmetric encryption for 1000s of years. Asymmetric is, however, a new player. In the 1970s, multiple Asymmetric keys were developed, including Diffie-Hellman (DH - 1976) and RSA (Rivest, Shamir and Adleman - 1977).

  - **Asymmetric Encryption uses 2 keys: A Public Key and a Private Key (Key Pair).**
    - Your **Public Key** is publicly available.
      - Used by others to encrypt messages sent to you. Since the key is asymmetric, the cipher text can't be decrypted with your public Key.
    - Your **Private Key** - You keep this safe.
      - You use it to decrypt messages sent with your public key.
    - Also used for digital signatures, slightly reversed.
    - You encrypt with your private key and the recipient decrypts with your public key.

- **Prime Number Factorization:**
  - Factoring large Prime numbers using a one-way factorization - It is easy to multiply 2 numbers, but hard to discern the 2 numbers multiplied from the result.
  - 1373 x 8081 = 11095213 - It will be hard to tell which numbers were multiplied to get 11095213.
  - Between 1 and 10,000 there are 1229 prime numbers, and strong encryption uses much higher prime numbers.

- **Discrete Logarithms:**
  - Another one-way function - this one uses Logarithms, which is the opposite of exponentiation.
  - 5 to the 12th power = 244140625 but asking 244140625 is 5 to the what power is much harder.
  - Discrete Logarithms apply the concept to groups, making them much harder so solve.

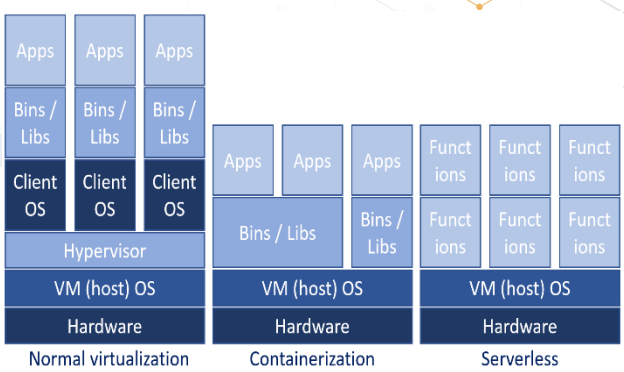
- **RSA cryptography**
  - New keypair from **very** large prime numbers - creates public/private key pair.
  - Used to exchange symmetric keys, it is slow, and the algorithm was patent protected (1977-1997 - 20 years).
  - Asymmetric, 1094-4096bit key, Considered secure.
  - **RSA-704** uses these 2 prime numbers, remember I said LARGE prime numbers were factorized:
    8143859259110045265727809126284429335877899002167627883200
    9141724293243601330041167020032408287779702524999
    9091213529597818878440658302600437485892608310328358720428
    5121689604115286409333678249507883679567568061 41
  - They then produce this result, and while this number is known, figuring out the 2 prime numbers is very difficult:
    7403756347956171282804679609742957314259318888923128908493
    6232638972765034028266276891996419625117843995894330502127
    5853701189680982867331732731089309005525051168770632990723
    96380786710086096962537934650563796359

- **Diffie–Hellman (DH)** key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols.
  - It is one of the earliest practical examples of public key exchange implemented within the field of cryptography.
  - The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel.
    - This key can then be used to encrypt subsequent communications using a symmetric key cipher.
- **Elliptic Curve Cryptography (ECC)** is a one-way function that uses discrete Logarithms applied to elliptical curves. Much stronger per bit than normal discrete Logarithms.
  - Often found on low-power devices since they can use shorter key lengths and be as secure.
  - Patented, so less used since it is patented and costs money to use, 256-bit ECC key is just as strong as a 3,072-bit RSA key.
- **ElGamal** is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems.
- **DSA** (Digital Signature Algorithm) uses a different algorithm for signing and encryption than RSA, yet provides the same level of security. Key generation has two phases.
  - The first phase is a choice of *algorithm parameters* which may be shared between different users of the system, while the second phase computes public and private keys for a single user.
  - DSA is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption.
- **Knapsack** (Merkle–Hellman knapsack cryptosystem) is one-way.
  - The public key is used only for encryption, and the private key is used only for decryption, making it unusable for authentication by cryptographic signing.
  - No longer secure.

- **Other cryptographic solutions :**
  - **Microservices:**
    - There is no single definition for microservices. A consensus view has evolved over time in the industry. Some of the defining characteristics that are frequently cited include:
    - Services in a microservice architecture (MSA) are often processes that communicate over a network to fulfill a goal using technology-agnostic protocols such as HTTP.
    - Services are organized around business capabilities.

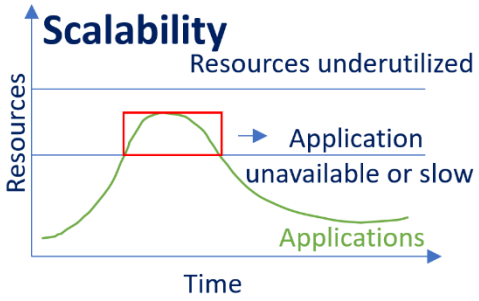
- Services can be implemented using different programming languages, databases, hardware and software environments, depending on what fits best.
- Services are small in size, messaging-enabled, bounded by contexts, autonomously developed, independently deployable, decentralized and built and released with automated processes.
- A microservice is not a layer within a monolithic application (for example, the web controller, or the backend-for-frontend). Rather it is a self-contained piece of business functionality with clear interfaces, and may, through its own internal components, implement a layered architecture.

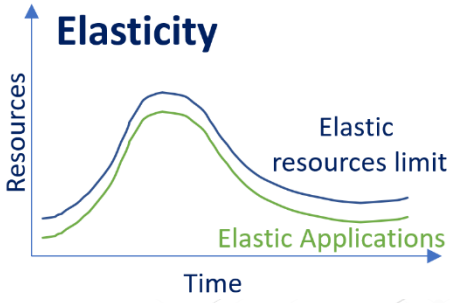
- **Containerization (OS-level virtualization):**
  - Removing redundant OS elements on a VM.
  - Applications are placed in containers. They only have the required resources needed to support that application.
  - They use a shared OS and unlike normal applications they can only see their container's content and the devices assigned to the container.



  - **Pros:**
    - Portability, scalability, deployment speed, enhanced security, easy to manage, cost-effective (between 10 and 100 times more application density per server than normal virtualization).

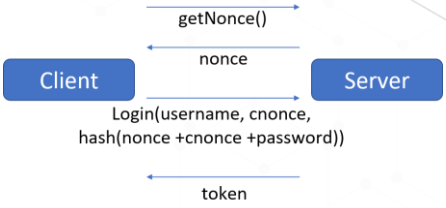
- **Serverless (Function as a Service (FaaS)):**
  - Similar to microservices, each function is made to work independently and autonomously.
  - Does not hold resources in volatile memory; computing in short bursts with the results persisted to storage.
  - **Pros:**
    - Cost is based on actual use. When the app is not in use, no compute resources are used.
    - Elasticity vs. Scalability.
      - → Elasticity; resources expand or contract based on the need.
      - → Scalability; we scale resources to meet expected needs.





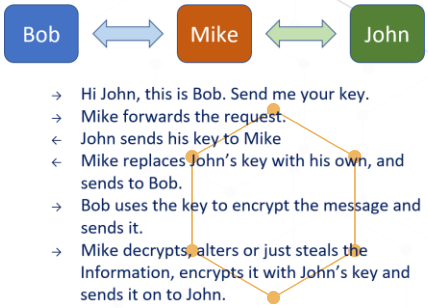
- **Hash Functions** (One-Way Hash Functions) are used for **Integrity**:
  - A **variable-length plaintext** is hashed into a **fixed-length value** hash or MD (Message Digest).
  - It is used to prove the Integrity of the data has not changed. Even changing a comma in a 1000-page document will produce an entirely new hash.
  - **Collisions:** When 2 hashes of different data provide the same hash. It is possible, but very unlikely.
  - **MD5** (Message Digest 5):
    - 128bit Fixed-Length hash, used very widely until a flaw was found making it possible to produce collisions in a reasonable amount of time.
    - While not a chosen-text collision, it is still a collision.
    - Still widely used.
  - **MD6** (Message Digest 6):
    - Was not used for very long; was supposed to replace MD5, but SHA2/3 were better.
    - It was in the running for the SHA3 race but withdrawn due to flaws.
  - **SHA1** (Secure Hash Algorithm 1):
    - 160bit Hash Value.
    - Found to have weak collision avoidance, but still commonly used.
  - **SHA2** (Secure Hash Algorithm 2):
    - Considered collision resistant.
    - Somewhat used now, relatively new.
  - **SHA3** (Secure Hash Algorithm 3):
    - Finalized in August 2015.
  - **HAVAL** (Hash of Variable Length):
    - The Message Digest (MD) length is variable (128, 169, 192, 224, 256bits).
    - Uses the MD design principles but is faster.
    - Not widely used.
  - **RIPEMD:**
    - Developed outside of defense to ensure no government backdoors.
    - 128, 256, 320bit hashes.
    - Not widely used.
    - No longer secure.
  - **RIPEMD160:**
    - Redesigned, fixing flaws of RIPEMD.
    - 160bit hashes.
    - Not widely used.
    - Considered secure.
  - **Salt (Salting):**
    - Random data that is used as an additional input to a one-way function that "hashes" a password or passphrase.
    - Salts are very similar to nonces.
    - The primary function of salts is to defend against dictionary attacks or a pre-compiled rainbow table attack.

- **Nonce:** (arbitrary number that may only be used once).
  - It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.
  - They can also be useful as initialization vectors and in cryptographic hash function.



- **Cryptographic Attacks**
  - **Steal the Key:** Modern encryption being so difficult to break, it is easier to recover the private key.
    - Law enforcement does this when they get search warrants, to recover the private key from the PC or phone of someone charged with a crime.
    - Attackers do this by gaining access to your system or key repository; they can then decrypt your data.
  - **Brute Force:**
    - Uses the entire key space (every possible key); with enough time, any plaintext can be decrypted.
    - Effective against all key-based ciphers except the one-time pad; it would eventually decrypt it, but it would also generate so many false positives that the data would be useless.
  - **Key stretching:** Adding 1-2 seconds to password verification.
    - If an attacker is brute forcing password and needs millions of attempts, it will become an unfeasible attack vector.
  - **Digraph attack:** Similar to frequency analysis/attacks, but looks at common pairs of letters (TH, HE, IN, ER).

  - **Man-in-the-Middle Attack (MITM):**
    - The attacker secretly relays and may alter communication between two parties, who believe they are directly communicating with each other.
    - The attacker must be able to intercept all relevant messages passing between the two victims.
    - They can alter the information, just steal it or inject new messages.



  - **Session Hijacking** (TCP Session Hijacking):
    - An attacker takes over a web user's session ID and masquerades as the authorized user.
    - Once the session ID has been accessed, through session prediction the attacker pretends to be the user, and as that user, can do anything the user is authorized to do on the network.

- **Social Engineering**
  - Much easier than breaking the key is convincing the key holder to hand it over to the “help desk”.
  - **FREE ICECREAM!**
    - A very successful social engineering attack was a Pen-Test company driving up in front of a company office with "Free Ice Cream” and company logo signs on an ice cream van.
    - The employees had to enter their username and password to ‘prove’ they were real employees. They were rewarded with an “approved" message and got their free ice cream.
    - The Pen-Testers got 90%+ of the employees’ usernames and passwords from those who were there that day.

- **Rainbow Tables:**
  - Pre-made list of plaintexts and matching ciphertexts.
  - Often Passwords and matching Hashes, a table can contain 1,000,000s of pairs.
- **Known Plaintext:**
  - You know the plaintext and the ciphertext and using those, you try to figure out the key.
- **Chosen Plaintext:**
  - Similar to Known Plaintext, but the attacker chooses the plaintext, then tries to figure out the key.
- **Adaptive Chosen Plaintext:**
  - Same as Chosen Plaintext, the attacker “adapts" the following rounds dependent on the previous rounds.
- **Meet-in-the-Middle:**
  - A known plaintext attack, the intruder has to know some parts of plaintext and their ciphertexts used to break ciphers which have two or more secret keys for multiple encryptions using the same algorithm.
- **Known Key** - (Not really known, because if it was, the attacker would have the key).
  - The attacker knows 'something' about the key, making it easier to break.
  - The password could be exactly 8 characters, first character has to be upper case and last has to be a number.

- **Differential Cryptanalysis:**
  - Tries to find the “difference" between the related plaintexts; if the plaintexts are only a few bits different, can we discern anything? Can we see non-randomness?
  - The same bit should have a 50/50 chance of flipping; areas where this is not so can be a clue to the key.
- **Linear Cryptanalysis:**
  - A type of known plaintext attack where the attacker has a lot of plaintext/ciphertext pairs created with the same key.
  - The attacker studies the pairs to learn information about the key used to create the ciphertext.
- **Differential Linear Cryptanalysis** is Differential and Linear Cryptanalysis combined.
- **Side Channel Attacks:**
  - Attackers use physical data to break a crypto system. This can be CPU cycles, power consumption while encrypting/decrypting, ...
- **Implementation Attacks:**
  - Some vulnerability is left from the implementation of the application, system or service.
  - It is almost always easier to find a flaw in the system than to break the cryptography.
  - Is the key stored somewhere in plaintext? Is the key stored somewhere not very secure? Is anything stored in memory?
- **Key Clustering:**
  - When 2 different Symmetric Keys used on the same plaintext produce the same ciphertext, both can decrypt ciphertext from the other key.
- **Pass the Hash**
  - If an attacker obtains a hashed password, they can gain access to the system by using the stolen hash and the user ID.
- **Kerberos exploitation**
  - **Overpass the Hash** or Pass the Key.
    - Similar to PtH but used when NTLM is disabled on a network.
    - Even when NTLM is disabled, the systems generate an NTLM hash and store it in memory.
    - The attacker requests a TGT with the user's hash to gain access to network resources.
  - **Pass the Ticket:**
    - The attackers attempt to collect tickets held in the lsass.exe process.
    - The attackers then inject the ticket impersonating the user.
  - **Silver Ticket:**
    - The attacker uses the NTLM hash of a service account to make a ticket-granting service (TGS) ticket.
    - Service accounts use TGS tickets instead of TGT tickets.

        - The silver ticket gives the attacker all the privileges granted to that specific service account.
    - **Golden Ticket:**
        - The attacker gains access to the hash of the Kerberos service account and can create any tickets they want within Active Directory.
        - The account signs and encrypts all Kerberos tickets on a domain with a hash of its own password.
        - The password never changes, meaning the hash also never changes.
    - **Kerberos Brute-Force:**
        - Attackers can guess passwords and usernames by using the Python script kerbrute.py on Linux or Rubeus on Windows because Kerberos will report whether a username is valid or not.
    - **ASREPRoast:**
        - Used to identify users who do not have Kerberos pre-authentication enabled.
        - Pre-authentication can help to prevent password guessing attacks.
        - If pre-authentication is not enabled disabled, the attacker sends an authentication request to the KDC.
        - The KDC replies with a TGT, encrypted with the client's password.
        - This enables the attacker to decrypt the ticket and the client's password using offline attacks.
    - **Kerberoasting:**
        - The attacker collects encrypted TGS tickets (because these are for service accounts, it is TGS rather than TGT).
        - When enough are collected, the attacker can try to decrypt them offline.
        - Services running in the context of user accounts would use a TGS ticket.
        - The attacker is trying to find users that don't have Kerberos pre-authentication enabled on their accounts.

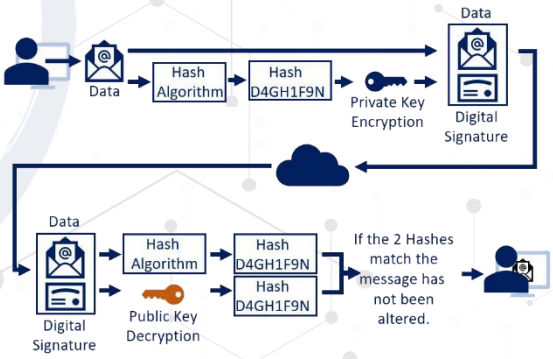
- **Fault injection**
    - The attacker is trying to compromise the integrity of cryptographic devices by introducing external faults.
    - Active side-channel attacks, trying to stress the device.
    - Power (high/low), temperature, and light are all potential factors.

- **Implementing Cryptography:**
  - **PKI** (Public Key Infrastructure):
    - Uses Asymmetric and Symmetric Encryption as well as Hashing to provide and manage digital certificates.
    - To ensure PKI works well, we keep the private key secret.
    - We also store a copy of the key pair somewhere central and secure (key repository).
    - We have policies in place that require 2 Security Administrators to retrieve the key pair (if only 1 person did it, chances of key compromise would be higher).
    - If users lose their private key and if no key repository is kept, anything encrypted with the public key is inaccessible.

    - **Key Escrow:**
      - Keys are kept by a 3rd party organization (often law enforcement).

  - **Digital Signatures:**

    *Provides **Integrity** and **Non-Repudiation**.*
    I want to send an email to Bob.
    - *My email is Hashed, the hash is encrypted with my private key (the encrypted Hash is my Digital Signature), I attach the signature to the email and send it.*
    - *Bob receives it, he generates a hash, and decrypts my signature with my public key. If the hash he generated and the hash he unencrypted match, the email is not altered.*



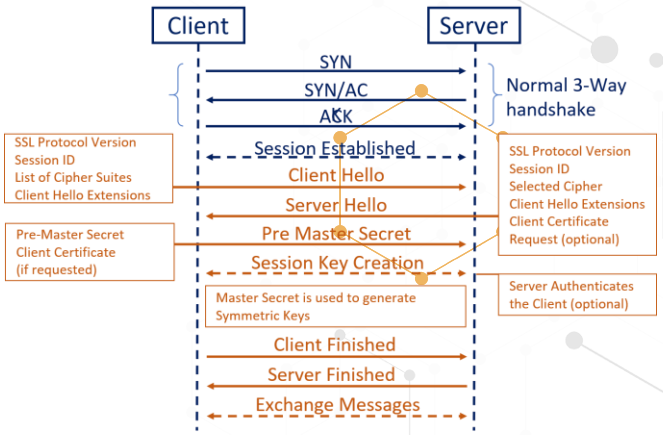
    - **Digital certificates** are public keys signed with a digital signature.
      - Server based - SSL for instance – is assigned to the server (stored on the server).
      - Client based - Digital Signature – is assigned to a person (stored on your PC).
      - **CA** (Certification Authority):
        - Issues and revokes certificates.
        - Can be run internally in your organization or in public (Verisign or GoDaddy, for instance).
      - **ORA** (Organizational Registration Authorities):
        - Done within an organization.
        - Authenticates the certificate holder prior to certificate issuance.

- **CRL** (Certification Revocation List):
  - → Maintained by the CA.
  - → Certificates are revoked if a private key is compromised, if an employee leaves the organization, etc.
  - → Server side, starting to be replaced by OCSP (client/server-side hybrid).
- **OCSP** (Online Certification Status Protocol):
  - → Client/server hybrid, better balance, faster, keeps lists of revoked certificates.

- The **Clipper chip** was a chipset that was developed and promoted by the United States National Security Agency (NSA) as an encryption device that "secured" voice and data messages with a built-in backdoor.
  - It was intended to be adopted by telecommunications companies for voice/data transmission but was abandoned after public outcry and was later found to have many security flaws (it used Skipjack).

- **MAC** (Message Authentication Code) – The exam uses MAC for several concepts; it will be spelled out which one it is.
  - Hash function using a key.
  - CBC-MAC, for instance, uses Cipher Block Chaining from a symmetric encryption (like DES).
  - Provides integrity and authenticity.
- **HMAC** (Hashed Message Authentication Code) combines a shared key with hashing.
  - A pre-shared key is exchanged.
  - The sender uses XOR to combine the plaintext with a shared key, then hashes the output using a hashing algorithm (Could be HMAC-MD5 or HMAC-SHA-1).
  - That hash is then combined with the key again, creating an HMAC.
  - The receiver does the same and compares their HMAC with the sender's HMAC.
  - If the two HMACs are identical, the sender is authenticated.
- **SSL** and **TLS** – Confidentiality and Authentication for web traffic.

  Cryptographic protocols for web browsing, email, internet faxing, instant messaging, and VOIP. You download the server's digital certificate, which includes the site's public key.
  - **SSL** (Secure Socket Layer) - Currently on v3.0.
    - Mostly used for web traffic.



- **TLS** (Transport Layer Security) - More secure than SSL v3.0.
  - Used for securing web traffic (less common).
  - Used for internet chat and email client access.

- **IPSEC** (Internet Protocol Security):

  Set of protocols that provide a cryptographic layer to IP traffic (IPv4 and IPv6). IPv4 was designed for secure research/military networks, but that is not how we use it now (bolt on security). IPSEC is often used for VPNs (Virtual Private Network) - local feel/security traffic over the internet.

  - **AH** and **ESP** - Can be used together or separately.
    - **AH** (Authentication Header):
      - → Provides Authentication and Integrity for each packet.
      - → Does NOT provide confidentiality (think of it as a digital signature for data).
      - → Protects against "replay attacks."
    - **ESP** (Encapsulation Security Payload):
      - → Provides confidentiality.
      - → It can provide Authentication and Integrity.
  - **SA** (Security Association):
    - Simplex one-way communication (Like a walkie talkie).
    - Can be used to negotiate ESP or AH parameters.
    - If 2 systems use ESP to communicate, they need 1 SA for each direction (2 total).
    - If they use AH and ESP, they will use 4 SAs (2x2).
    - A unique 32 bit SPI (Security Parameter Index) is used to identify each SA connection.
  - **ISAKMP** (Internet Security And Key Management Protocol):
    - Manages the SA creation process and key exchange mechanics.
  - **Tunnel mode** encrypts and authenticates the entire package (including headers).
  - **Transport mode** only encrypts and authenticates the payload. This is used for systems that speak IPSEC.
  - **IKE** (Internet Key Exchange):
    - IPSEC can use different types of encryption and hashes. For example, it can use MD5 or SHA-1/2 for integrity and 3DES or AES for confidentiality.
    - IKE negotiates the algorithm selection process.
    - The 2 sides of an IPSEC tunnel will normally use IKE to negotiate to the highest and fastest level of security, selecting AES over single DES for confidentiality if both sides support AES, for example.

- **Pretty Good Privacy** (**PGP**):
  - Provides privacy and authentication for data communication. Can provide confidentiality, integrity, authentication, and non-repudiation.
  - PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions, and to increase the security of e-mail communications.
  - PGP uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms.
  - Uses a Web of Trust model to authenticate digital certificates, if you trust me, you trust everyone I trust.
- **MIME** (Multipurpose Internet Mail Extensions) provides a standard way to format email, including characters, sets, and attachments.
- **S/MIME** (Secure/MIME) uses PKI to encrypt and authenticate MIME-encoded email.
  - The client or client's email server (called an S/MIME gateway) can perform the encryption.

Physical Security

*As part of physical security, we also design **"Design-in-Depth"** into our plan.*

- **Preventative Controls:**
  - Prevents action from happening – Tall fences, locked doors, bollards.
- **Detective Controls:**
  - Controls that detect an attack (before, during or after) – CCTV, alarms.
- **Deterrent Controls:**
  - Controls that deter an attack – fences, security guards, dogs, lights, Beware of the Dog signs.
- **Compensating Controls:**
  - Controls that compensate for other controls that are impossible or too costly to implement. We may not be able to move our datacenter or change the foundation, but we can add absorbers under the sub-floor, in the racks, …
- **Administrative Controls:**
  - Controls that give us administrative framework – compliance, policies, procedures.

- **Perimeter defense:**
  - **Fences** (Deterrence, Preventative):
    - Smaller fences such as 3ft. (1m) can be a deterrence, while taller ones, such as 8ft. (2.4m) can be a prevention mechanism.
    - The idea of the fences is to ensure entrance/exits from the facility happen through only a few entry points (doors, gates, turnstiles).

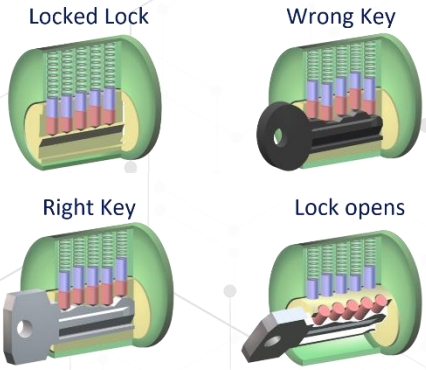
  - **Gates** (Deterrence, Preventative):
    - Placed at control points at the perimeter.
    - Used with the fences to ensure access only happens through a few entry points.
    - **ASTM Standard:**
      - Class I Residential (your house)
      - Class II Commercial/General Access (parking garage).
      - Class III Industrial/Limited Access (loading dock for 18-wheeler trucks).
      - Class IV Restricted Access (airport or prison).
  - **Bollards** (Preventative):
    - Used to prevent cars or trucks from entering an area while allowing foot traffic to pass.
    - Often shops use planters or similar; it looks prettier but achieves the same goal.
    - Most are static heavy-duty objects, but some cylindrical versions can also be electronically raised or lowered to allow authorized traffic past a "no traffic" point. Some are permanent fixtures and can be removed with a key or other unlock functions.

  - **Lights** (Detective and Deterrence):
    - Lights should be used to fully illuminate the entire area.
    - Lights can be static, motion activated (static) or automatic/manual Fresnel lights (search lights).
    - Measured in lumen - 1 lumen per square foot or lux - 1 lumen per square meter more commonly used.

- **CCTV** (Closed Circuit Television) (Detective, Deterrence) - used to monitor the facility's perimeter and inside it.
  - **Older cameras** are analog and use video tapes for storage (often VHS); quality is often bad, unclear.
  - **Modern cameras** are digital and use CCD (Charged Couple Discharge); also use a **DVR** (Digital Video Recorder).
  - Organizations may have retention requirements either from policies or legislation that require a certain retention of their video (this could be bank ATM, data center or entry point footage).

  - Cameras can be either static or non-static (automatic or manual).
    - We have all seen the spy or heist movies where they avoid them by knowing the patterns and timers.
    - This risk can be mitigated with a randomizer or pseudo randomizer, we want to ensure full coverage.

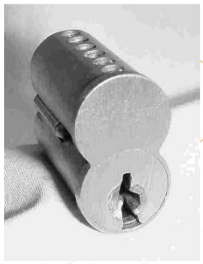
- **Locks** (Preventative):
  - **Key locks:**
    - Requires a physical key to unlock; keys can be shared/copied.
    - **Key Bitting Code** (How far the key is bitten down for that section.) – Can be copied and replicated without the key from either the numbers or a photo of it.



    - **Pin Tumbler Lock** (or Yale lock) – A lock mechanism that uses pins of varying lengths to prevent the lock from opening without the correct key.
    - **Lock Picking** - with a lock pick sets or bumping, opening a lock without the key.
      - → Any key lock can be picked or bumped, how long it takes depends on the quality of the lock.
      - → Lock pick sets lift the pins in the tumbler, opening the lock.

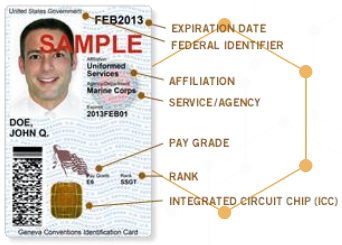
- **Lock Bumping** - Using a shaved-down key that matches the lock, the attacker "bumps" the key handle with a hammer or screwdriver which makes the pins jump, then the attacker quickly turns the key.
- **Master Keys** open any lock in a given area or security zone.
  - → Both who has them and where they are kept should be very closely guarded at all times.
- **Core Key** is used to remove a lock core in "interchangeable core locks."
  - → An interchangeable core, or IC, is a compact keying mechanism in a specific figure-eight shape.
  - → Relies upon a specialized "control" key for insertion and extraction of the core.
  - → Should be kept secure and access should be very restricted.

Interchangeable core lock



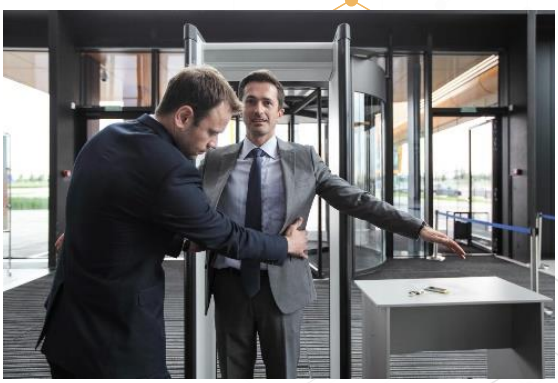
- **Combination Locks:**
  - Not very secure and have limited accountability even with unique codes.
  - Should be used for low security areas.
  - Can be Dial type (think safe), Button or Keypad.
  - Very susceptible to brute force, shoulder surfing and are often configured with weak security (I know of a good deal of places where the code is the street number).
  - Over time, the buttons used for the code will have more wear and tear.
  - For 4-number PIN where 4 keys are used, the possible combinations are no longer 10,000, but 256; if 3 keys, then 81 options.

- **Smart Cards** (contact or contactless):
  - They contain a computer circuit, using ICC (Integrated Circuit Card).
  - **Contact Cards** - Inserted into a machine to be read.
    - This can be credit cards you insert into the chip reader or the DOD CAC (Common Access Card).
  - **Contactless Cards** - can be read by proximity.
    - Key fobs or credit cards where you just hold it close to a reader.
    - They use an RFID (Radio Frequency Identification) tag (transponder) which is then read by an RFID Transceiver.



- **Magnetic Stripe Cards:**
  - Swiped through a reader, no circuit.
  - Very easy to duplicate.
- **Tailgating/Piggybacking:**
  - Following someone authorized into an area you are not authorized to be in.
  - Often combined with Social Engineering.
  - It is easy to do if your reason for being there seems plausible.
  - Bring a lot of food, a cake, and some balloons, have on clothes, ID badge and tools that a repairman would, the options are endless.
- **Mantrap:**
  - A Mantrap is a room with 2 doors; Door 1 must close completely before Door 2 can be opened.
  - Each door has a different authentication method (something you know, something you have, something you are).
  - They can at times use weight sensors - Bob weighs 220lbs (100kg), the weight measured by the pressure plate is 390lbs (177kg), someone is probably in the room with Bob. Door 2 won't open until Bob is confirmed alone in the Mantrap with a cart of old servers, normally done by the cameras in the trap.

- **Turnstiles** (Preventative, Deterrence):
  - Also prevents tailgating, by allowing only 1 person to enter per Authentication (think like in US subway systems or amusement park entries, but for secure areas they are often floor to ceiling turnstiles with interlocking blades).
- **Contraband Checks** (Preventative, Detective, Deterrent):
  - Often seen in airports, courthouses, intelligence offices or other higher security facilities.
  - Checking what you are bringing in or out of the building to ensure nothing dangerous gets in or anything confidential gets out.
  - With technology becoming much smaller, these are less effective when it comes to data theft; it is easy to hide a microSD memory card, which can contain up to 1TB+ of data per card.



- **Motion Detectors** (Detective, Deterrence):
  - Used to alert staff by triggering an alarm (silent or not).
  - Someone is here, did an authorized person pass the checkpoint?
    - IF yes, then log the event and do nothing else
      IF no, then alert/alarm.
  - Basic ones are light-based - They require light, making them not very reliable.
  - **Ultrasound, Microwave, Infrared or Laser** (*pew-pew!!*)
    - Active sensors, they send energy (sound, wave or light).
    - If the sound takes less time to return or the pattern it receives back is altered, it means someone is somewhere they should not be.
    - Photoelectric motion sensors send a beam of light to a sensor, if broken the alarm sounds. These are the *pew-pew* lasers and sorry, no, they are not green or red and they are rarely visible.

- **Perimeter Alarms:**
  - Door/window sensors – these are the thin strips around the edges of either or contact sensors.
    - If opened, an alarm sounds; if broken, same effect.
    - Can be circumvented, but they are part of a layered defense.
  - Walls, windows, doors, and any other openings should be considered equally strong.
  - Walls are inherently stronger; the rest need compensating measures implemented (locks, alarms, sensors).
  - Glass is normally easy to break, but can be bullet and/or explosion proof, or have a wire mesh in the middle.
  - Plexiglass can also be used, as it is stronger and does not shatter, but can be melted.
  - Door hinges should always be on the inside (or hidden in the door).
  - Just like the turnstiles and mantraps, doors (and in some cases windows) should be designed to allow safe exit from the building in case of an emergency. Often there is a "Panic Bar" that opens the door, but they are also connected to alarms that sound when opened (clearly labeled Emergency Only - Alarm WILL Sound).

- **Walls, Floors, and Ceilings:**
  - In line with our layered defense strategy, the strong security encountered in getting to a data center does nothing if there is a crawl space that an attacker can use.
  - We need to secure all possible ways into our Data Center or other secure location.

- Walls should be "slab to slab" (from the REAL floor to the REAL ceiling); if sub-flooring or sub-ceilings are used, then they should be contained within the slab to slab walls.
- Walls, floors, and ceilings should be made of materials (where it makes sense) that are secure enough for that location, e.g. don't have sheetrock around your Data Center because I can cut that with a knife.
- Walls, floors, and ceilings should have an appropriate fire rating.
  - So should your doors, but walls, floors and ceilings are more often overlooked.
  - This is to protect the Data Center from outside fire and just as well the rest of the building from a Data Center fire.

- **Guards** – (Deterrent, Detective, Preventative, Compensating)
  - Guards can serve many diverse purposes for an organization.
  - They can check credentials/ID Cards, monitor CCTV cameras, monitor environmental controls (HVAC), react to incidents, act as a deterrent, and so much more.
  - **Professional Guards** - Professional training and/or schooling; armed.
  - **Amateur Guards** - No professional training or schooling; armed.
  - **Pseudo Guard** - Unarmed guard.
  - Guards should have a very clear set of rules and regulations.
  - Social engineering attacks are common and should be prevented with training to raise awareness.

- **Dogs** (Deterrent, Detective, Compensating):
  - Most often used in controlled, enclosed areas.
  - Liability can be an issue.
  - Dogs are trained to corner suspects and attack someone who's fleeing. People often panic when they encounter a dog and run.
  - Even if they're in a secure area, the organization may still be liable for injuries.
  - Can also be internal authorized employees walking out the wrong door or trying to take a shortcut.
  - They panic and the dog attacks.

- **Restricted Work Areas and Escorts.**
  - To track and funnel authorized visitors, we can use visitor badges, visitor logs, and escorts.
  - Non-electronic visitor badges are easy to make copies of and easy to fake.
  - Electronic can be just a cheap re-programmable magnetic strip (like for hotel rooms, easy to copy). Make sure they have a short window of use, or more secure individually printed ones for each visit, and only used once.
  - The return of all badges and physical sign-out should be enforced when the visitor leaves.
  - When a vendor is coming to repair, install or remove something in your facility, they need to be checked in and escorted from the entry point to where they are going to work by an employee, and the employee should stay with the vendor until the work is completed.
  - The vendor's employees should already have passed a security check when they were hired; the vendor is liable.
  - This sounds and is boring, but it is more likely to prevent the vendor from compromising your security than if they were free to roam the facility and the data center unsupervised.

- **Site Selection, Design, and Configuration:**

  Before building a new facility, it is very important to do proper research and planning. Multiple factors need to be considered, but for the exam you need to think about the security ones.

  - **Site Selection:**
    - **Greenfield** - Not built on yet, undeveloped land.
    - **Topography** - the physical shape of the landscape - hills, valleys, trees, streams. Most often used at military sites where they can leverage (sometimes by altering) the topology for better security.

    - **Utilities** - How reliable is the power, the internet in the area?
    - **Crime** - How high are the crime rates in the area? How close are the police?

- **Site Design:**
  - **Site Marking:**
    - Do not advertise your data center's (or other critical) locations.
    - The more nondescript and boring the building is, the less attention it gets (security through obscurity).
    - A determined attacker can obviously find the information, but the harder you make it, the less your chances are of being compromised.
      - → Example: Don't name your credit card processing server creditcard001.

- **Shared Tenancy and Neighbors**
  - Sharing your building with someone else poses other security risks; the people working at or visiting those organizations are already past the perimeter.
  - Their bad security posture can be a risk to yours.
  - Attackers can set up base right next door, they can eavesdrop and attack on your wireless without causing much suspicion.
  - Think of the many movies with bank robberies or great heists where they go through a neighbor's wall, ceiling or floor.
  - These all have a basis in reality from real robbers who did just that.

- **Wiring Closets**
  - If shared, the other tenants have access to your network. You can lock it down, but it is still a big security concern. I have seen a place where one tenant had all their equipment bolted to the wall, but the wires were exposed; it would be easy to attach a sniffer to that.

- **Demarc -** Point of Demarcation (POD):
  - Where the ISP (Internet Service Provider) terminates their phone/internet lines and your network begins; most buildings only have one.
  - When shared, it is a security concern that other tenants have access. Can they access your equipment?
  - IPv4 is not inherently secure and ISP connections are not either. You must add the security on your end.
  - It is desired to have strong Access Control for the Demarc. If not possible, find another location. (IAAA)
  - For secure sites or sites that need high uptime, it is common to have multiple Demarcs from multiple ISPs. How segmented and secure each Demarc is depends on your information security posture.

- **Server Rooms and Data Centers:**
  - Many Data Centers were designed for our past requirements and not how much data we move today.
  - Pop-up server rooms are built when we outgrow our current Data Center and we bolt-on somewhere in the building that was NOT built for that purpose.
  - They often lack proper walls, floors, ceilings, flood prevention; bolted-on and not designed-in is less secure.
  - I have seen a bolt-on server room where there were showers and bathrooms just above it. What a fun day they would have if the floor/ceiling started leaking.
  - **Data Center Build or Expansion:**
    - How much HVAC (Heating, Ventilation and Air Conditioning) do we need for now/future use?
    - Which natural events do we need to factor in for where we are (e.g. hurricanes, floods, tornadoes)?
    - Do we have enough Power for current/future use; is the grid stable? Are blackouts or brownouts common? Brownout = drop in voltage (lights flicker). Blackout = power is interrupted completely.
    - **Power:**
      - → What size of generators do we need?
      - → How large of a **UPS** (Uninterruptible Power Supply) do we need? Huge battery bank also ensures consistent voltage.
    - **Fire Suppression:**
      - → Dry pipe vs. wet pipe.
      - → Halon/Chemical/FM200.
      - → Fire extinguishers.

- **Media Storage and Locations:**

  Where and how you store your offline data/media and (preferably) offsite is dictated by internal policies, procedures, and compliance requirements.

  - All storage media should be encrypted (Data at Rest).
  - Media (often tape) should be stored at an offsite facility.
  - The facility should be climate controlled (temperature and humidity) less strict than a data center, standards still apply.
    - Tape will deteriorate at a certain temperature just as disks will corrode at a certain humidity.
    - The storage facility should be secure, licensed, and bonded (both for transport and storage), lost data is just as lost, but they are liable.

  - Multiple incidents have happened when this was done, and break-ins relieved the employees of the tapes, which in many cases were NOT encrypted. Welcome to $10,000, $100,000 or $1,000,000 fines/lawsuits or loss of revenue from the bad publicity hit. (Data at Rest should always be encrypted).

- **Asset Tracking:**

  Keeping an accurate inventory of all our assets is important; we can't protect what we don't know we have. We covered this a little in our risk analysis section, but other than identifying the assets, we also should have it as part of our technology refresh cycle to record the Asset Serial Number, Model Number, and often an internal Asset ID.

  - **Hardware Hardening:**
    - On our servers - we harden the server.
      - Apply all patches, block ports not needed, delete default users, … most places are good about this.
    - Workstations are often overlooked.
  - **Disabling the USB Ports**, CD drives and any other port that can introduce malware to our network.
    - Physically: Disabled on motherboard or port itself blocked, easy to bypass - not very secure.
    - Logically: Locked in Windows services or through AD (Active Directory) is not easy to bypass (if done right) - more secure.

Environmental Controls

- **Electricity**

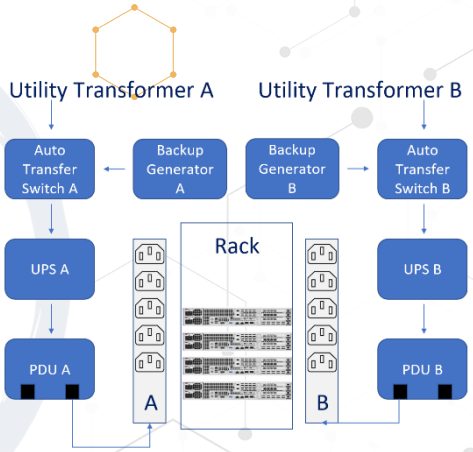
It is important to have clean, reliable power for our servers, disk arrays, network equipment.

- Loss of power can affect our availability and the Integrity of our data.
- Nothing can be accessed and power fluctuations can damage hardware and corrupt data.


Data Center Batteries for UPSs


Data Center PDUs

- **Power Fluctuation** Terms:
  - **Blackout** - Long loss of power.
  - **Fault** - Short loss of power.
  - **Brownout** - Long low voltage.
  - **Sag** - Short low voltage.
  - **Surge** - Long high voltage.
  - **Spike** - Short high voltage.



- **Surge Protectors**, **UPSs** and Generators are used to get clean power.
  - **Surge Protectors** - Protect equipment from high voltage.
  - **UPSs** (Uninterruptible Power Supplies):
    - Ensure constant clean power to the systems.
    - Have large battery banks that take over in the event of a power outage, they also act as surge protectors.
- **Generator:**
  - Fueled generators are programmed to manually or automatically (preferred) kick in during a power outage event.
  - Will run as long as they have fuel, must be maintained.
  - **PDU** (Power Distribution Unit) can be in rack or not.
- **EMI (Electromagnetic Interference)**
  - Disturbance generated by an external source that affects an electrical circuit by electromagnetic induction, electrostatic coupling or conduction.
  - In our world this includes circuits, power cables, network cables, ...
  - Often, this is an issue with network cables that are not shielded properly or run too closely to power cables. Magnetism from one cable “crosses” over to a neighbor cable (crosstalk).
  - This can impact the **Integrity** (data corruption), **Confidentiality** (data sniffed), and **Availability** (data unavailable).

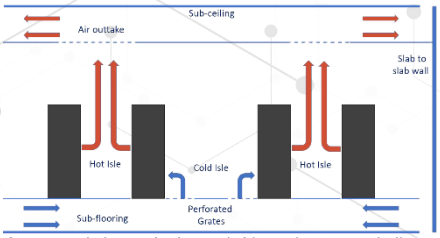
- Crosstalk is avoided with proper cable management and by using STP (Shielded Twisted Pair) cables, not UTP (Unshielded Twisted Pair) cables.
- Power cables should never be run close to copper data cables.
- Fiber optic cables are used when it makes sense (not susceptible to EMI or sniffing, since they are glass).
- On the exam, if asked for the cheapest secure cables, fiber > copper, while not as cheap they are way more secure.

- **HVAC:**
  - **Heat**:
    - Many data centers are kept too cold, the last decade's research has shown it is not needed.
    - Common temperature levels range from 68–77 °F (20–25 °C) - with an allowable range of 59–90 °F (15–32 °C).
    - Keeping a data center too cold wastes money and raises humidity.

Vendor Data Center temperature recommendations:

Vendor	Low (C°/F°)	High (C°/F°)	Optimal
Cisco	18/64.4	27/80.6	-
Google	-	-	26.7/80
Dell	24+/Upper 70 F°	26+/Lower 80 F°	
HP	18/64.4	27/80.6	
IBM	18/64.4	27/80.6	
Oracle	21/70	23/74	22/72

  - **Pressure**:
    - Keeping positive pressure keeps outside contaminants out.
  - **Humidity:**
    - Humidity should be kept between 40% and 60% rH (Relative Humidity).
    - Low humidity will cause static electricity and high humidity will corrode metals (electronics).
  - **Drains**:
    - Many data centers use subflooring where water and contaminants (mostly dust) can gather. If an HVAC unit malfunctions, it can leak water.
    - It is important to have sensors in the subfloor for both water and dust, and to regularly vacuum the space.



Servers, switches and other rackable equipment are built with air intake and exhaust facing the hot and cold aisles. Servers have intake in the front and exhaust in the back and switches are often reserved.

- **Static Electricity:**
  - Can be mitigated by proper humidity control, grounding all circuits, using antistatic wrist straps and work surfaces.
  - All personnel working with internal computer equipment (motherboards, insert cards, memory sticks, hard disks) should ground themselves before working with the hardware.

Antistatic shoes.
Not the prettiest thing I ever saw, but effective!

Antistatic wrist wrap.

- Heat, Flame, and Particle/Smoke Detectors:
  All used for detecting fires or potential fires, they are connected to warning lights, sirens, and suppression systems.
  - Heat Detectors:
    - Configured to trigger when a certain threshold is exceeded (Rise of 10° F in < 5 minutes or rising above 90° F).
  - Smoke Detectors: (Ionization or Photoelectric):
    - Ionization detectors have a small radioactive source which creates a small electric charge.
    - Photoelectric uses LED (Light Emitting Diode) and a photoelectric sensor that produces a small charge while receiving light.
    - Both trigger when smoke or any higher particle density interrupts the radioactivity or light.
  - **Flame Detectors:**
    - Flame detectors detect infrared or ultraviolet light emitted by fire.
    - They require line of sight to detect the flame.

Personnel Safety, Training and Awareness

Personnel safety *is* ***always*** *most important.*

- You may like your servers more but save the co-worker first. **(This is very testable).**
- Organizations should have clear policies, procedures, and standards for evacuations.
- Evacuation routes should be clearly marked and known by all staff.
- Meeting points should be established (can also stop staff from reentering the building looking for a coworker who is already somewhere else outside).

- Evacuation roles are established; a pre-appointed person ensures all staff is out of the building and another is the meeting point leader.
- Plans are in place for disabled employees (elevators are not working at this time).
- Fire/evacuation drills are held quarterly or annually.
- All exit doors (or special emergency-only doors) have the "panic bar" (crash bar).
- Just like in the data center, we have warning sirens and lights throughout the building to alert staff to exit.

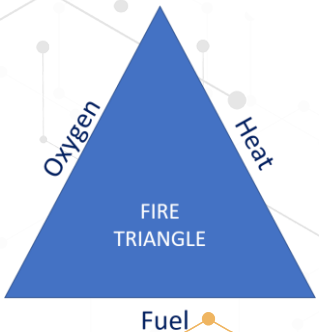
- **Personnel Safety:**
  - **Early Warning Systems** (Duress Warning Systems):
    - Warning systems are used to provide immediate alerts to personnel/people in the event of emergencies, severe weather, threat of violence, chemical contamination, ...
    - Duress systems are mostly local and can use overhead speakers, sirens or automated communications like email, pagers, text messages or automated phone calls.

ABCD Fires and Suppression

- **Fire suppression**

Fire suppression *is done by removing one of the 3 requirements a fire has.*

- A fire needs Oxygen, Heat, and Fuel to burn.
  - Removing any of the 3 will put the fire out.
  - **Removing Oxygen** is done by replacing the oxygen in the room with something else or covering the fire so the burning material doesn't have oxygen access (Halon, FM200, Argon).
  - **Removing Heat** is done by adding chemicals or water to the fire, cooling it down.
  - **Removing Fuel** is rarely done since the fuel is our equipment.



- **Fire Classes:**
  - Remember that the certification is **International**, so answer appropriately for the question's scenario, not for where you live.
  - Answer all questions from a **management or risk advisor level** and in a **top-down** security organization.
  - Appropriate fire suppression and extinguishers should be deployed in all areas.

American	European	UK	Australian/Asian	Fuel/heat source
Class A	Class A	Class A	Class A	Ordinary combustibles
Class B	Class B	Class B	Class B	Flammable liquids
	Class C	Class C	Class C	Flammable gases
Class C	Unclassified	Unclassified	Class E	Electrical equipment
Class D	Class D	Class D	Class D	Combustible metals
Class K	Class F	Class F	Class F	Cooking oil or fat

- **Automatic Fire Suppression Systems:**
  - **Water:**
    - Removes the "heat" leg of the fire triangle by lowering the temperature.
    - Is the safest suppression agent, but for Data Centers:
      - Water + hardware = dead hardware.
    - Electricity could always be cut before water is used.
    - **Sprinkler Systems:**
      - Sprinklers have different types of bulbs for different temperatures.
      - Should be connected to alarm/warning sirens and lights.
      - Each sprinkler head is independent; it will trigger if the temperature for that bulb is met.
      - **Wet Pipe:** Sprinkler heads are closed. The pipes for the sprinkler system have water until the sprinkler.
      - **Dry Pipe:** Sprinkler heads are closed.
        - → The pipe contains compressed air and a valve that stays shut as long as the air is present.
        - → Used in areas where frost might be an issue or where water can be an issue.
        - → I have seen dry pipe in a data center; scary for me but was built in as a last resort.
      - **Deluge:** Sprinkler heads are open.
        - → Similar to Dry Pipe, but sprinkler heads are open, a deluge valve holds water back, normal air in pipes.

Temperature		Color of liquid alcohol inside bulb
°C	°F	
57	135	Orange
68	155	Red
79	174	Yellow
93	200	Green
141	286	Blue
182	360	Purple
227	440	Black
260	500	

- **Pre-Action:**
  - → Single interlock: Water released into pipes when the fire alarm goes off and when head opens.
  - → Double interlock: Similar to Dry Pipe, water is not released until fire alarm sounds off and the sprinkler is open.

- **Gases:** All gas fire suppression systems must have a visible and audible countdown so staff can exit the area.
  - **CO_2**:
    - Should only be used in unmanned areas.
    - It is colorless and odorless and causes people in it to pass out and then die.
    - Staff working in an area where CO_2 is used should be properly trained in CO_2 safety.
  - **Halon 1301** has been the industry standard for protecting high-value assets from fire since the mid-1960s.
    - It has many benefits; it is fast-acting, safe for assets, and requires little storage space.
    - It is no longer used widely because it depletes atmospheric ozone and is potentially harmful to humans.
    - In some countries legislation requires the systems to be removed; in others it is OK to use them still (with recycled Halon), but systems have not been installed since 1994 (The Montreal Accord).

    The Montreal Accord (197 countries) banned the use and production of new Halon. A few exceptions for "essential uses" include things like inhalers for asthma and fire suppression systems in submarines and aircraft.
  - **Halon Replacements** (other halocarbons and inert gases):
    - **Argon**: 50% Argon gas and 50% Nitrogen gas
    - **FE-13** (Fluoroform): Low toxicity, low reactivity, and high density. Breathable up to 30% concentration.
    - **FM-200** (HFC-227ea): Low toxicity, most are designed to provide a concentration of 6.25-9% heptafluoropropane.

Agent	Primary Ingredient	Applications
FM-200 (HFC 227)	Heptafluoropropane	Electronics, medical equipment, data centers, medical record rooms, server rooms, telecommunications rooms.
IG-01	Argon	Same applications as FM-200, less Class B style hazards.
Carbon Dioxide (CO_2)	Carbon Dioxide	Non-occupied control rooms, transformer vaults, live electrical equipment.
FE-13	Fluoroform	Electronics, medical equipment, data centers, medical record rooms, server rooms, telecommunications rooms.
Wet Chemical	Potassium carbonate	Commercial kitchens
Regular Dry Chemical	Sodium bicarbonate	Gasoline, propane and solvents, live electrical equipment, flammable liquids
Foam	Synthetic detergent, polysaccharide, fluoroakyl suffaccant	Flammable liquids
Halotron 1	2,2-dichloro-1,1,1-trifluoroethane	Live electrical equipment, flammable liquids
Water Mist	Water	All Classes of Fire (A,B,C,F) Ordinary flammables (Paper, wood, cloth), Flammable liquids, Kitchen Fires (K,F Class), Electrical Fires

- **Inergen:** Nitrogen (52%), Argon (40%), and Carbon Dioxide (8%); the air is still breathable, but the fire is put out.
  - → Breathing is more labored due to increased CO_2.

- **Fire Suppression:**
  - **Fire Extinguishers:**
    - A fire extinguisher is an active fire protection device used to extinguish or control small fires, often in emergency situations.
    - All portable fire extinguishers should be marked with the type of fire they are designed to extinguish.
    - Never use a fire extinguisher on a fire it was not intended for.
    - Use the **PASS** method to extinguish a fire with a portable fire extinguisher:
      - **P**ull the pin in the handle.
      - **A**im at the base of the fire.
      - **S**queeze the lever slowly.
      - **S**weep from side to side.

    - **Soda-Acid Extinguishers** mix a solution of water and sodium bicarbonate with an acid (in a vial, which is broken) to expel pressurized water onto a fire.
    - **Dry Powder Extinguishers** (sodium chloride, graphite, ternary eutectic chloride).
      - Lowers the temperature and removes oxygen in the area.
      - Primarily used for metal fires (sodium, magnesium, graphite).
    - **Wet Chemical** (potassium acetate, potassium carbonate, potassium citrate).
      - Extinguishes the fire by forming an air-excluding soapy foam blanket over the burning oil and by the water content cooling the oil below its ignition temperature.

Final Points to Remember

- **Virtualization**
  - Virtualization also poses new vulnerabilities because the technology is new-ish and very complex.
  - Clients on the same host should be on the same network segment (Internal/DMZ). A host should never house both zones.
  - Clients should be logically separated on the network like physical servers would be (HR, Accounting, IT VLANs).
- **Cloud Computing**

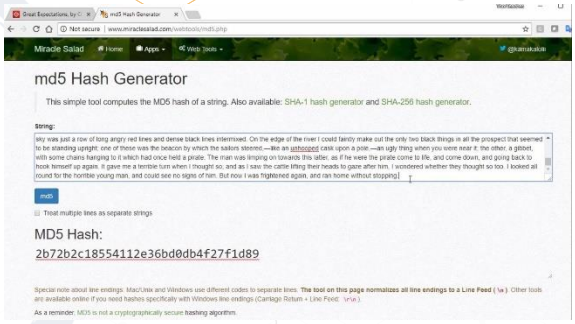
  (There is no 'Cloud', it is just another computer somewhere else).
  - When we use cloud computing we build or outsources some part of our IT Infrastructure, storage, applications.
  - This can be done for many good reasons, but most are cost related. It is cheaper to have someone larger or more specialized in that one area doing it for us.
  - As with any other outsourcing, make sure you have the right to audit, pen test (clearly agreed upon criteria), conduct vulnerability assessment, and check that the vendor is compliant with your industry and the standards you adhere to.
- **Web Architecture and Attacks**
  - The internet is a very complex place. Security is often added on as an afterthought and not designed in as it should be.
  - On top of that the internet was never intended to be what it is today; it was originally designed to be a secure closed network.
- **Mobile Security**
  - The more external devices we connect, the more complex policies, procedures, and standards we need.
  - **Mobile devices** are really anything "mobile" – External hard disks, USB drives, CDs, laptops, cell phones, …
  - Most internal threats are not malicious people. They just don't know any better, didn't think about it or figured they wouldn't get found out.
  - **Good security** policies should lock down USB ports, CD drives, network ports, wireless networks, disable autorun on media, use full disk encryption, have remote wipe capabilities, raise user awareness training on where (if anywhere) mobile devices are allowed. (Defense in Depth)

- **Cryptography**
  - For the exam, what you need to know is that cryptography helps us:
    - Keep our secrets secret (**Confidentiality**) ← This is what most people think all cryptography does.
    - Keep our data unaltered (**Integrity**).

        - Provide a way to verify (**Authentication**) our Subjects; it can also provide **non-repudiation**.
    - Cryptography has been used for thousands of years to keep secrets secret.
    - Encryption should be strong enough to be unbreakable or at least take a very long time to break; there obviously needs to be a balance between Confidentiality and Availability.
    - **Modular Math:**
        - Cryptography uses a lot of modular math.
        - For the exam you need to know what it is, but you don't need to know how to do it.
        - Numbers "wrap around" after they reach a certain value (modulus), which is also why it is called clock math.

      Adding "X" (24) to "E" (5) = "C" (3) - The English alphabet wraps around after the 26th letter (modulus).
- **Hashing**

  Just 1 bit changed completely changes the hash. Using Great Expectations (Charles Dickens 1867 Edition again, 4 pages at font size 11, 1827 words, 7731 characters).

    - **Hash#1** is the original
    - **2b72b2c18554112e36bd0db4f27f1d89**
    - **Hash#2** is with 1 comma removed
    - **21b78d32ed57a684e7702b4a30363161**
    - Just a single "**.**" added will change the hash value to **5058f1af8388633f609cadb75a75dc9d**

  ***Remember**: variable-length input, fixed-length output.*
- **Physical Security**
    - Both **Mantraps** and **Turnstiles** should be designed to allow safe evacuation in case of an emergency. (***Remember that people are more important to protect than stuff.***)

- **What we covered in the third CBK Domain.**

In this chapter we talked about how we protect our assets.

- ✓ How the domain has 3 major knowledge areas (prior to the 2015 exam update, each had their own domain).
  - ✓ **Security Architecture and Design:**
    - The common security models.
    - The architecture, design, virtualization, cloud, and solutions we use to protect our assets.
    - How computers work (basics) and how they are logically segmented.
    - Threats to our applications, systems, and devices.
  - ✓ **Cryptography:**
    - The history of cryptography, types of encryption, hashes, cryptography attacks, and digital signatures.
  - ✓ **Physical Security**
    - Site and facility secure design principles, perimeter defense, HVAC, power, and fire suppression.