MSDS 7349 Data and Network Security Exam 1 (MidTerm)

Shanqing Gu

Due Day: 07/01/2018

Rename this file using this format: Shanqing Gu_7349_MidTerm.docx

For each multiple-choice question and each answer choice, write 3-5 sentences explaining why that answer choice either is, or is not, correct

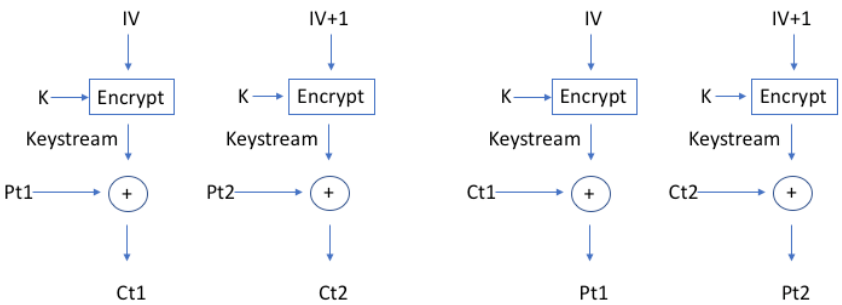
Question 1- to 15 (each is 5 points):

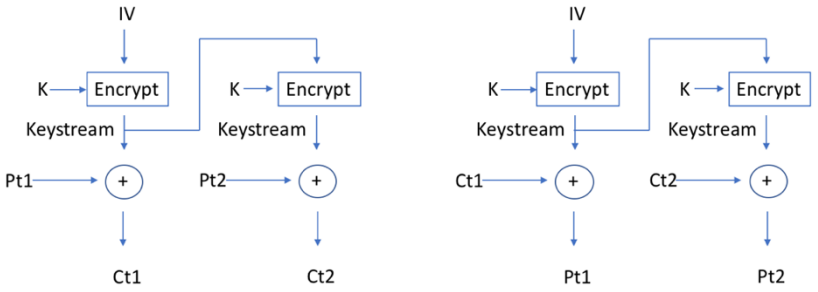
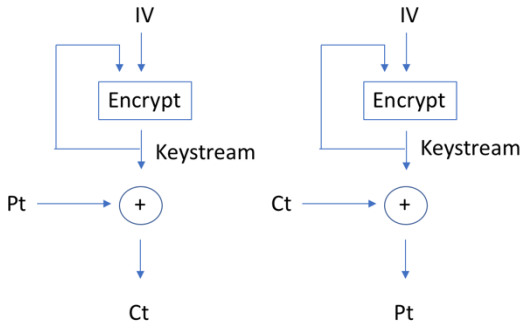
Q1: Answer (**B**)
Explain Other Choices:

In cryptography, a cipher is an algorithm for performing encryption or decryption (correct answer B). The word "cipher" comes from Arabic *sifr* which means "empty", "nothing", "no digit", "naught", or "zero" (answer C). Commonly, "cipher" is interchangeable with "code" (answer D) because both are a set of steps to encrypt a message. However, the concepts are distinct in cryptography, especially in classical cryptography. A code replaces whole words with symbols while ciphers replace individual letter with other letter or symbols. A cipher will manipulate the letters of a plaintext while a code will manipulate the whole words. The encrypted massage (answer A) is called the ciphertext while a message is called the plaintext.

Q2: Answer (**D**)
In Q2, the diagram is to help you explain the operation. The diagrams are already in the online videos. After drawing the diagram, you add the sentences that explain the mode itself

The operations for Counter Mode (answer A), Output Feedback Mode (answer B) and Stream Mode (answer C) all create a keystream to be XORed (**Exclusive or** or **exclusive disjunction** is a logical operation that outputs true only when inputs differ) with the plaintext for encryption. Therefore, the correct answer for this question should be answer D (all of the above) and exclude answer E (none of the above).

Counter (CTR) mode (answer A): Plaintext blocks XORed with encrypted counter, which is incremented for each subsequent block. Similar characteristics to OFB but allows a random-access property during decryption. Typical application involves general-purpose block-oriented	

transmission and use for high-speed requirements.	
Output feedback (OFB) mode (answer B) makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to generate the ciphertext. Because of the symmetry of the XOR operation, encryption and decryption are exactly the same.	
Stream ciphers and stream modes of operation (answer C) worked by generating a keystream. For encryption, this key stream is XORed with the plaintext in order to generate the ciphertext. For the decryption, the keystream is XORed with ciphertext in order to generate the plaintext.	

Q3: Answer (**B**)
Explain Other Choices:

The correct answer is answer B (Trust). A trust relationship is a relationship involving multiple entities to trust each other having or not having certain properties (trust-assumptions). It is the inherent ability for hosts to communicate within a network design. Trust and risk are opposites; Security is based on enforcing and limiting trust. Within subnets, trust is based on Layer 2 forwarding mechanisms. Between subnets, trust is based on Layer 3+ mechanisms.

Cryptography Encryption and Decryption (answer A) is that the sender encrypts a message with the recipient's public key. Secure use of cryptography requires trust. While secret key cryptography can ensure message confidentiality and hash codes can ensure integrity, none of this works without trust.

The Authentication (answer C), which is the foundation of all security on the internet. Authentication is the assurance that the communicating entity is the one that it claims to be. It consists of peer entity authentication and data-origin authentication.

Public key certificates (answer D) are digital documents issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. A public key certificate

represents a trust edge from the CA to the owner of the certified public key. Public key infrastructure (PKI) is functioning as a chain of trust in security architecture.

Digital signatures (answer E) allow the senders to "sign" messages with their private keys and verify the messages come intact from claimed senders. In situations where there is not complete trust (answer B) between sender and receiver, something more than authentication (answer C) is needed. The most attractive solution to this problem is the digital signature (answer E).

Q4: Answer (**D**)
Explain Other Choices:

The correct answer is answer D (all of the above).

Security is concerned with threats to survival. Human security is the concept to understand global vulnerabilities.

Compared to traditional security, the war and the threat to use force is only part of the security equation (answer A), and not necessarily the most important.

From the contemporary view, human security: (1) is people-centered rather than protecting a state's boundaries, people, institutions and values (answer A); (2) has broader scopes of protection including environmental pollution, infectious diseases, and economic deprivation (answer B); (3) involves not only governments, but a broader participation of different actors; (4) not only protects, but also empowers people and societies as a means of security (answer C).

Q5: Answer (**D**)
Explain Other Choices:

The correct answer is D (all of the above), which means that all three modes of operation allows for the decryption on each block can be performed in parallel.

For Counter mode (answer A), it turns a block cipher into a stream cipher by generating the next keystream block with encrypting successive values of a counter. This mode is well suited to operate on a multi-processor machine where blocks can be encrypted and decrypted in parallel.

For Cipher Block Chaining (CBC) Mode (answer B), each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block. Its main drawbacks are that encryption is sequential and cannot be parallelized. For the decryption, a plaintext block can be recovered from two adjacent blocks of ciphertext. As a consequence, decryption can be parallelized.

For Electronic Codebook (ECB) Mode (answer C), the message is divided into blocks and each block is encrypted and decrypted separately. ECB naturally supports encryption and decryption operation in parallel.

Q6: Answer (**D**)
Explain Other Choices:

The correct answer is answer D. The secure hash function has three properties: preimage resistance (answer A), second preimage resistance (answer B), and collision resistance (answer C).

For preimage resistance (answer A) with one-way property, x=the preimage of h for hash value h=H(x) with H to include many-to-one mapping and h to include multiple preimages. Given a hash value h, it is computationally infeasible to find any message m such that *h=hash(k, m)*.

Second preimage resistance (answer B) is a weak Collison resistance. Given block x, it is computationally infeasible to find $y \neq x$ with H(y)=H(x).

Collison resistance (answer C) is a strong Collison resistance. Given two messages m1 and m2. It is computationally infeasible to find H(k, m1) = H(k, m2), where k is the hash key. This is the hardest standard for a hash function to attain.

Q7: Answer (**A**)
Explain Other Choices:

The correct answer is answer A (hacker). An intruder (answer C) might do some port scanning, gain access to the target system, exploit the unpatched vulnerability in the system/network, and try to know the intrinsic details of the system he compromised.

Comparatively, a hacker, one who uses programming skills to gain illegal access to a computer network or file, may follow the same pattern as intruder but will delete/modify or copy the data from the system he compromised or may use this system as a platform to launch further attacks.

Identity thief (answer B) steals your personal information and use it to commit crimes.

Cyber-terrorist (answer D) is a person that uses the internet to destroy or damage computers for political reasons like the air traffic control towers, electrical plants or telecommunication infrastructure.

Q8: Answer (**D**)
Explain Other Choices:

The correct answer is answer D (all of the above). E-mail privacy (answer A), software privacy (answer B), intellectual property and copyrights (answer C) are all ethical issues facing the use of technology in business today.

Business companies of every size face a multitude of ethical issues and balance the need for technology with elements of privacy and security.

For e-mail privacy (answer A), it is important to create policies regarding to email communications in the workplace. If the policy is vague, it may not protect the employer and employee and bring ethical issues.

For software privacy (answer B), the illegal copying of software (software privacy) is considered one of the ethical issues on cyberspace with its impact on the global economy. Copies of software should be made only with proper authorization.

For intellectual property rights and copyrights (answer C), computing professional are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas and work, even in cases where the works has not been explicitly protected by copyright, patent, etc. (refer to ACM code).

Q9: Answer (**A**)
Explain Other Choices:

The correct answer is answer A (Scalability). Scalability is the property where any extracted subsequence should pass the test for randomness. Any test applicable to a sequence can be applied to subsequences extracted at random.

PRNGs are derived through algorithms which should provide high degree of randomness. Uniformity, scalability and consistency are all checks for randomness of a PRNG. PRNGs use an input known as "seed" which is usually generated using a TRNG. Therefore, answer C (a shared initialization vector) is not correct.

For pseudorandom number generator (PRNG), when considering the possibility of not knowing initial conditions, backward predictability is used with a long-known sequence can return those conditions and also predict some sequences in accurate guesses. A stream of pseudorandom number must be unpredictable (forward and backward unpredictability) in order to be classified as "random". Therefore, answer B (backward predictability) is not correct.

Since only answer A is correct, answers D and E are not correct.

Q10: Answer (**A**)
Explain:

Integrity is that sender and receiver want to ensure message not altered (in transit or afterwards) without detection. Only encryption is not enough in this case, and the solution is to add some kind of checksum (hash) to the message before it is encrypted.

Answer A (Hash function) is correct. Hash function H can (1) accept a variable-length block of data M as input and produces a fixed-size hash value, (2) produce evenly distributed and apparently random outputs, and (3) protect data integrity. Even just one changed bit gives a completely different result (avalanche effect).

For private key operation (answer B), public key and private keys are a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact

transformations performed by the algorithm depend on the public or private key that is provided as input.

For Symmetric key operation (answer C), symmetric key encryption is a type of encryption that makes use of a single key for both the encryption and decryption process. Some of the encryption algorithms that use symmetric keys include: AES. Blowfish, DES, Triple DES, Serpent and Twofish.

Q11: Answer **(C)**
Explain:

An assessment of the strength of an encryption method is based on: (1) algorithm complexity, (2) the secrecy of the key, (3) key length (correct answer C), (4) the initialization vectors (IVs) and (5) how all of these parts work together within the cryptosystem.

Larger keys provide more secure encryption. Key length is measured in bits. 128-bit RC4 encryption is $3x10^{26}$ times stronger than 40-bit RC4 encryption. In most cases, the shared secret key (answer A) is used with the RC4 secret-key cipher to encrypt the actual messages between the server and browser.

The strength of encryption is determined by the key size. Asymmetric algorithms require large keys. For example, 1024-bit for low-, 2048-bit for medium- and 4096-bit for high-strength asymmetric key. Symmetric keys are smaller: 256-bit keys give you strong encryption.

It is also hard to use 'keep algorithm details secret' (answer B) strategy to increase the strength of a specific cipher.

Therefore, the correct answer is answer C (use a key with a larger number of bits).

Q12: Answer (**D**)
Explain:

For answer A (use both linear and non-linear functions), the idea of mixing linear and non-linear operations in order to obscure the relationship between the plaintext, ciphertext and key is called confusion and is an important principal of cipher design. Most notably, the use of a highly nonlinear found function ensures a high resistance to linear attacks.

For answer B (use one or two more rounds than the minimum to achieve randomness), the essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. The greater the number of rounds, the more difficult it is to perform cryptanalysis, even for a relatively weak F.

For answer C (have good avalanche properties), the algorithm should have good avalanche properties. In general, it means that a change in one bit of the input should produce a change in many bits of the output. A more stringent version of this is the strict avalanche criterion (SAC) [WEBS86], which states that any output bit j of an S-box should change with probability ½ when any single input bit I is inverted for all I, j.

Therefore, the correct answer is answer D (all of the above) which includes confusion, number of rounds, and good avalanche properties for design of Function F.

Q13: Answer (**D**)
Explain:

For answer A (Grain 128-A), it is a new member in the family of Grain stream ciphers which uses a 128-bit key and the size of the IV is 96 bits. Grain 128a consists of two large parts: Pre-output function and MAC. The pre-output function has an internal state size of 256-bit with two registers of size 128-bit (NLFSR and LFSR). The MAC supports variable tag lengths. Grain 128a is very well suited for hardware environments (Reference: M. Agren et al., *A New Version of Grain-128 with Authentication* http://skew2011.mat.dtu.dk/proceedings/A%20New%20Version%20of%20Grain-128%20with%20Authentication.pdf)

For answer B (Hummingbird 2), it is an encryption algorithm with a 128-bit secret key and a 64-bit initialization vector. Authenticated Encryption with Associated Data (AEAD) is a method of using Hummingbird that encrypts /decrypts a payload and also authenticates any associated data (AD) that travels alongside the ciphertext such as the nonce and a packet header (Reference: Daniel Engels et al., https://eprint.iacr.org/2011/126.pdf)

For answer C (Keyak), Sponge-based AE schemes, as stateful extensions of the classical AEAD. This approach builds on an API-based syntax that allows a scheme to be used in the traditional stateless, nonce-based AEAD sense, but supports "sessions" for encrypting message-AD pairs in a stateful way (Reference: Damian Vizar, Tatra Mt. Math. Publ. 67 (2016), 167–190. DOI: 10.1515/tmmp-2016-0038).

Therefore, the correct answer is answer D which includes Grain 128-A, Hummingbird 2 and Keyak.

Q14: Answer (**D**)
Explain:

The correct answer is answer D (all of the above).

A public-key encryption scheme allows everyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt.

Security depends on the secrecy of the private key. It consists three algorithms: (1) key generation: Outputs a pair (pk, sk) where pk is a public key and sk is a private/secret key; (2) Encryption: Takes the public key pk and a plaintext m as input, and outputs a ciphertext c (Answer A: The public key encrypts only, so it must take the plaintext as input); (3) Decryption: Takes the secret key sk and a ciphertext c as input, and outputs a plaintext m (Answer B: The private key is used only for decryption of ciphertext encrypted with the public key).

For answer C (*In RSA in theory, once the keys are calculated, if the 'public key' is kept secret and the 'private key' is made public, the cipher is not secure*), private and public keys cannot be swapped and are not always of the same type (depending on the cryptosystem used). In RSA, as the public key is calculated from the private key, switching them means your formerly private key is now the public key, and anybody could quite easily generate the formerly public key which you now use as your private key. Therefore, switching public/private keys in RSA makes RSA unsafe.

Q15: Answer (A)
Explain:

A message authentication code (MAC), the keyed hash function, is a function of the message and a secret key that produces a fixed-length value used to authenticate a message. The MAC value, generated and verified using the same secret key, protects both a message's integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

If intruder could compute another massage (y) with same MAC (x) [i.e. MAC (y) = MAC (x)], intruder can modify the message (answer B) and insert new MAC (y) (answer A). The receiver will repeat the verification process and validate the signature. The receiver will not know that the message was not changed.

For source repudiation (answer C), source repudiation is the denial of transmission of message by source. In order words, the sender sends a message, and then later denies sending it or claims that the message that was sent was different. A digital signature is an authentication technique that also includes measures to counter repudiation by the source.

An attacker who alters the message will be unable to alter the associated secure MAC value (answer A) without knowledge of the secret key, noting that the verifying party knows who the sending party is because no one else knows the secret key.

Therefore, only message authentication code modification (answer A) can be mitigated by a secure message authentication code.

Q16 (6 points)

In probability theory, the birthday paradox concerns the probability of two people in a group sharing a birthday. The calculation shows that only 23 people needed for probability > 50%. Real-world applications (like using hash values as IDs) for the birthday paradox include a cryptographic attack called the birthday attack, which used this probabilistic model to reduce the complexity of finding a collision for a hash function.

For example, if we use a 16-bit hash code the level of effort required is only on the order of $\cong 2^{m/2}=2^{16/2}=2^8 = 64$ which is clearly not sufficient to withstand today's computational systems. The solution is to use long hash values (256-bit or greater, 512-bit common today) for preventing birthday paradox.

Assume the birthday paradox for variables of bit size n= 16, 32, 64, 128, 256, and 512, the following table contains a range of small probabilities.

	Hash out length (bit size)					
Probability	16-bit	32-bit	64-bit	128-bit	256-bit	512-bit
0.5	2^8	2^{16}	2^{32}	2^{65}	2^{129}	2^{257}

Q17 (7 points)

In Q17, for each layer (5 layers), pick one protocol. Then summarize the main tasks and features of that protocol. Therefore, you describe 5 different protocols.

	Layer Name	Security Protocol	Function
5	Application layer	S-RPC, DNSSEC, S-HTTP S-RPC (secure remote procedure call): based on DES encryption algorithm, uses public key scheme for encryption and vendor specific. DNSSEC (domain name system security): provide authentication and integrity of DNS answers, designed to protect against cache poisoning, uses public key scheme, but does not do encryption. Reference: Jonathan Spring. Monitoring cloud computing by layer, part 2. IEEE Security & Privacy (2011) 9:3. **DOI:** 10.1109/MSP.2011.57	Provide applications services to users and programs
4	Transport layer (TCP/UDP)	SSL, TLS, WTLS, SSH, SOCKS SSL (secure sockets layer)/TLS(transport layer security): encrypts client-server communication, used by protocols like https for security, server authentication to client mandatory, and client authentication to server optional. SSL/TLS handshake includes encryption negotiation, identification of server and/or client, key exchange. Reference: Mohammad Tanveer Khan, Review: Network Security Mechanisms and Cryptography. International Journal of Computer Science and Mobile Computing, Vol.6 Issue.7, July- 2017, pg. 138-146	Handles data-consistency functions, i.e., provides a reliable byte stream between two nodes on a network. TCP and UDP work at this level.
3	Network Layer (IP)	IPSec and GRE IPsec (internet protocol security): mutual node authenticates users, but requires L2TP, crypto implementation agnostic, client-to-client, or node-to-node, mandator for IPv6 implementation, does not work with NAT, unless NAT-Transversal (NAT-T) is used. GRE (generic route encapsulation): used to secure VPNs, creates a virtual point-to-point link with destination, support multicast protocols. Reference: P. Knight and C. Lewis. Layer 2 and 3 virtual private networks: taxonomy, technology, and standardization efforts. IEEE Communications Magazine (2004) 42 (6). **DOI:** 10.1109/MCOM.2004.1304248	Provides network addressing and routing and does so in such a way as also to provide a common address space across multiple lower-level protocols. This makes possible the interconnection of networks that characterizes the Internet. The IP protocol operates at this level.

2	Data Link layer (MAC)	IEEE 802.1x Point-to-point Protocol (PPP), Point-to-point tunneling protocol (PPTP), Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol, VPN, wireless network security, MPLS For L2F (Layer 2 forwarding), Not IP dependent, support ATM and frame relay, relies on PPP for authentication, used for VPNs and no encryption by itself. Reference: Jyh-Cheng Chen and Yu-Ping Wang. Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience. IEEE Communications Magazine (2005) 43 (12). **DOI:** 10.1109/MCOM.2005.1561920	This layer contains whatever IP will run over, e.g., Ethernet, token-ring, and Fiber Distributed Digital Interface (FDDI) networks. Individual network protocols, e.g., Ethernet, work at this level.
1	Physical layer	There are some security protocols like CLIMEX, but physical security controls can be implemented, and types of cabling used can make a difference. CLIMEX is a wireless physical layer security protocol based on clocked impulse exchange. Reference: Satyam Dwivedi, John Olof Nilsson, Panos Papadimitratos, Peter Handel. CLIMEX: A Wireless Physical Layer Security Protocol Based on Clocked Impulse Exchanges. https://arxiv.org/pdf/1708.04774.pdf	Not really part of the model, since TCP and IP, as protocols, deal with software rather than hardware. This layer is generally thought of as referring to all hardware under the Data Link Layer.

Q18 (6 points)

Bandwidth depletion and resource depletion attacks are two main classes of DDoS attacks.

(1) DDoS bandwidth depletion attack: it is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. Bandwidth attacks can be divided to flood attacks and amplification attacks. As being the first DDoS attack tool to be widely distributed and used, Trinoo is a bandwidth depletion attack tool that can be used to launch coordinated UDP flood attacks against one or many IP addresses.

(2) Resource depletion attack: it is designed to tie up the resources of a victim system. This type of attack can be divided to protocol exploit attacks and malformed packet attacks. Tribe Flood Network (TFN) is a DDoS attack tool that provides the attacker with the ability to wage both bandwidth depletion and resource depletion attacks.

Many potential approaches have been implemented to mitigate the attack. For example, resource pricing, many Intrusion Tolerant QoS Techniques and Intrusion Tolerant QoS systems.

Reference papers:

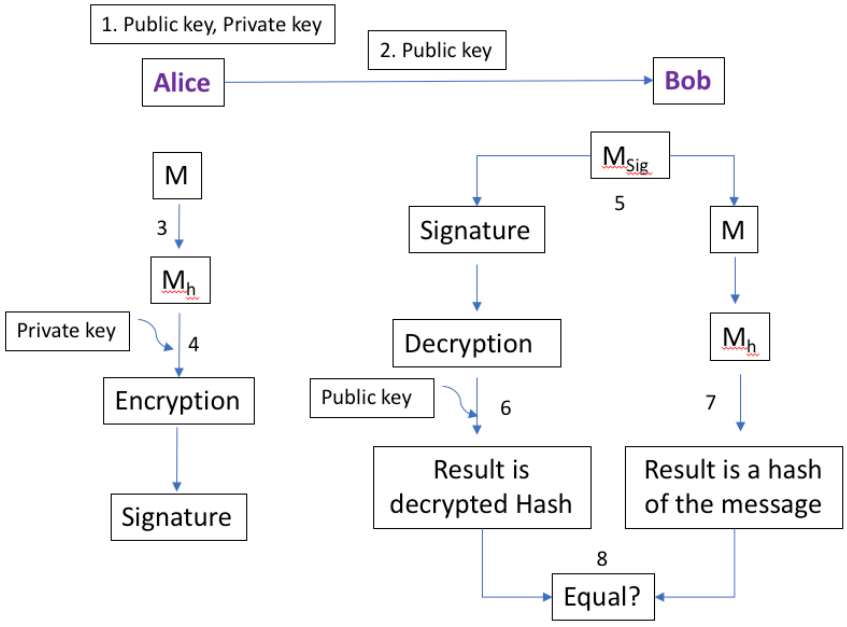
Christos Douligeris and Aikaterini Mitrokotsa. DDOS Attacks and Defense Mechanisms: A Classification Conference Paper · January 2004 DOI: 10.1109/ISSPIT.2003.1341092 · Source: IEEE Xplore

Christos Douligeris, Aikaterini Mitrokotsa. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks 44 (2004) 643–666. doi:10.1016/j.comnet.2003.10.003

Q19 (6 points)

A man-in-the-middle (MITM) attack happens when a communication between two systems is intercepted by an outside entity. Some common types of MITM attacks are: Email Hijacking, Wi-Fi Eavesdropping, Session Hijacking. MITM attacks can be prevented or detected by two means: authentication and tamper detection. Authentication provides some degree of certainty that a given message has come from a legitimate source. Tamper detection merely shows evidence that a message may have been altered.

Digital signature is one of the mechanisms to prevent or detect MITM attacks. It is based on a combination of public key encryption and one-way secure hash function algorithms.



Steps for Alice as the sender to create a digital signature:

1. Alice creates a public/private key pair.
2. Alice gives his public key to Bob;
3. Alice write a message to Bob and uses the document as input for a one-way hash function.
4. Alice encrypts the output as the hash of the message with his private key, resulting in the digital signature.

Steps for Bob as the receiver to verify the message is indeed from Alice:

5. Bob separates the received message into the original document and the digital signature.
6. Bob used Alice's public key to decrypt the digital signature, resulting in the original message digest.
7. Bob takes the original document and uses it as input to the same hash function that Alice uses, which results in a message digest.
8. Bob compares both of the message digests to see whether they match. If Bob's calculation of the message digest matches Alice's decrypted message digest, the integrity of the document the authentication of the sender is proven.