CS4331/CS5342 Network Security
Homework 2

Submitted By:
Ashlesha Malla
R#: R11904228

Q.1. What are the pros and cons of public-key cryptography (4 points)

- The pros of public-key cryptography are:

  a. The primary advantage of public-key cryptography is it is very secure. The key never needs to be transmitted or revealed to anyone.
  b. Public-key cryptography enables the creation of digital signatures, which can be used to verify the authenticity of a message or document.
  c. Since the sender is the only one with the private key, public-key cryptography allows for non-repudiation, which means that a sender cannot deny sending a message.

- The cons of public-key cryptography are:

  a. Public key encryption in this method is slow compared with symmetric encryption, which means that it is not suitable for decrypting bulk messages.
  b. It risks loss of private key, which may be irreparable. When you lose your private key, your received messages will not be decrypted.

Q.2. What are the properties of public key encryption? (4 points)

- The properties of public key encryption are:

  a. Separate keys are used for both encryption and decryption of the data.
  b. Confidentiality is ensured since messages encrypted with the public key can only be unlocked with the matching private key.
  c. A digital signature that provides authentication and confirms the sender's identity can be made with the private key.
  d. It is practically not possible to determine the decryption key but only given knowledge of the cryptographic algorithm and encryption.

Q.3. Describe the steps of public key encryption with example (4 points)

- Steps for Public key encryption:
  - Step1: Generate a pair of keys.
  - Step2: • keep the private key / secret key (SK) and distribute the public key PK).
  • Place PK in a public register or other accessible file.

- Step3: Bob encrypts the message with Alice's PK. Step4: Upon receiving the ciphertext (CT), Alice decrypt CT with SK.

Example:
Bob wants to send Alice an encrypted email. To do this, Bob takes Alice’s public key and encrypts his message to her. Then, when Alice receives the message, she takes the private key that is known only to her in order to decrypt the message from Bob.

Q.4. Which categories should be used to classify public key cryptography algorithms? (4 points)

- Following categories should be used to classify public key cryptography algorithms:

a. Encryption/Decryption (provide secrecy)
b. Digital signatures (provide authentication)
c. Key exchange (of session keys)
d. Some algorithms are suitable for all uses; others are specific to one
e. Either of the two related keys can be used for encryption, with the other used for decryption.

Algorithm	**Encryption/Decryption**	**Digital Signature**	**Key Exchange**
RSA	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No
Elliptic curve	Yes	Yes	Yes

Q.5. Write RSA encryption and decryption algorithms. Suppose the public key {e, n}, and private key {d, n} are given. (4 points)

- RSA Encryption Algorithm:
  Given a message M and a public key {e, n}, the RSA encryption algorithm works as follows:
  1. Create an integer m from the message M such that $0 \leq m < n$.
  2. Make the ciphertext c as c = m^e (mod n).
  3. Return the ciphertext c.

- RSA Decryption Algorithm:
  Given a ciphertext c and a private key (d, n}, the RSA decryption algorithm works as follows:
  1. Compute the plaintext p as p = c^d (mod n).
  2. Convert the plaintext p back into the original message M.
     • It should be noted that step 2 of the RSA decryption process is required since it is possible that the plaintext p and the original message M are different.
     • Any encoding or formatting strategy that was employed to change M into m in the RSA encryption algorithm can be used to change p back into M.

Overall, the RSA encryption and decryption algorithms are relatively simple to implement and provide a high level of security for data transmission. However, the security of the algorithm relies on the difficulty of factoring large numbers, so it's important to use sufficiently large key sizes to prevent attacks.

Q.6.What are the possible attacks exploiting RSA's properties? (4 points)

- The possible attacks exploiting RSA’s properties are:

  a. Mathematical Attack
  Attempts to factorize the modulus *n* to obtain the private key. This is the most direct attack on RSA. It becomes feasible if the modulus is not large enough or if weak primes are chosen.

  b. Timing Attack
  Takes advantage of differences in the time required for cryptographic procedures depending on the input. An attacker might deduce details about the private key by looking at these variations.

  c. Chosen Ciphertext Attack
  This type of attacks exploits properties of the RSA algorithm by selecting blocks of data. These attacks can be thwarted by suitable padding of the plaintext, such as PKCS1 V1.5 in SSL.

Q.7. What is meant by message authentication? (4 points)

- Verifying the validity and integrity of a message or data transmission is known as message authentication. It guarantees that communication has not been altered while in transit and that the sender listed on it is, in fact, the real one.

  Message authentication is concerned with:
  - protecting the integrity of a message
  - validating identity of originator
  - non-repudiation of origin (dispute resolution)

Q.8. What are the 3 approaches to achieve message authentication? (4 points)

- The three common approaches to achieve message authentication are:

  a. Message Encryption:
  Message encryption by itself also provides a measure of authentication.
  A. If symmetric encryption is used, then:
    1. Receiver knows sender that who must have created it.
    2. Since only sender and receiver know the key used.
    3. Known content cannot be altered.
  B. If public-key encryption is used:
    1. Encryption provides no confidence of sender
    2. Since anyone potentially knows public key

3. So, need to recognize corrupted messages

C. However, if

1. Sender signs message using their private key
2. Then encrypts with recipients' public key
3. Have both secrecy and authentication

But at cost of two public-key uses on message

b. Message Authentication Codes (MACs):
Message Authentication Code is the short piece of information that is used to authenticate a message, and to provide integrity and authenticity assurances on the message.

c. Digital signatures
A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software.

Q.9. What are the pros and cons of single-key cryptography? (4 points)

- The pros of single-key cryptography are:

a. Symmetric-key algorithms are typically faster than their asymmetric counterparts. This makes them well-suited for encrypting large amounts of data.
b. Comparing symmetric keys to those used in asymmetric encryption, they can be comparatively short.

- The cons of single-key cryptography are:

a. In symmetric-key cryptography, the key distribution to both parties must be done securely. The system's protection may be compromised if a third party manages to intercept the key while it is being transmitted.
b. Since the same key is used for both encryption and decryption, it's not possible to prove the origin of a message or verify the sender's identity.

Q.10. List and explain the requirements for a secure hash function (4 points)

a. can be applied to any sized message M
b. produces fixed-length output h
c. is easy to compute h-HM) for any message M
d. given h is infeasible to find x s.t. H(x)=h one-way property or preimage resistance
e. given x is infeasible to find x' s.t. H(x)=H(x) weak collision resistance or second pre-image resistant
f. infeasible to find any pair of x,x' s.t. H(x')-H(x) strong collision resistance

Q.11. What is the weakness of hash function? (4 points)

- The weaknesses of hash function are:

a. Some hash functions are susceptible to length extension attacks. An attacker can extend a hash value with additional data without knowing the original input.
b. Hash functions are vulnerable to collision attacks. A collision occurs when two different inputs produce the same hash value.
c. In certain situations, the output length of a hash function may be inadequate to provide a sufficient level of security.

Q.12. How many solutions to guarantee the integrity of hash function? (4 points)

- The solutions to guarantee the integrity of hash function are:

a. Message Authentication Codes (MACs)
Because it can guarantee that the message hasn't been altered, a message digest generated using a secret symmetric key is referred to as a message authentication code (MAC).
b. Digital Signature
When a digital signature is verified using the public key, it confirms that the message was indeed signed by the holder of the private key. It also ensures that the message has not been tampered with.

Q.13. Does hashes provide integrity? (4 points)

- Scenario 1:
• Scenario
  • Mozilla publishes a new version of Firefox on some download servers
  • Alice downloads the program binary
  • How can she be sure that nobody tampered with the program?
• Idea: use cryptographic hashes
  • Mozilla hashes the program binary and publishes the hash on its website
  • Alice hashes the binary she downloaded and checks that it matches the hash on the website
  • If Alice downloaded a malicious program, the hash would not match (tampering detected!)
  • An attacker can't create a malicious program with the same hash (collision resistance)
• Threat model: We assume the attacker cannot modify the hash on the website
  • We have integrity, as long as we can communicate the hash securely

Scenario 2:
• Scenario
  • Alice and Bob want to communicate over an insecure channel
  • David might tamper with messages
• Idea: Use cryptographic hashes
  • Alice sends her message with a cryptographic hash over the channel
  • Bob receives the message and computes a hash on the message
  • Bob checks that the hash he computed matches the hash sent by Alice
• Threat model: David can modify the message and the hash
  • No integrity!

Q.14. What is the definition and properties of message authentication code? (4 points)

- Two parts:
  - • KeyGen → K: Generate a key K
  - • MAC(K, M) → T: Generate a tag T for the message M using key K
  - • Inputs: A secret key and an arbitrary-length message
  - • Output: A fixed-length tag on the message

  Properties
  - • Correctness: Determinism
  - • Note: Some more complicated MAC schemes have an additional Verify(K, M, T) function that don't require determinism, but this is out of scope
  - • Efficiency: Computing a MAC should be efficient
  - • Security: existentially unforgeable under chosen plaintext attack

Q.15. What are the properties of HMAC? (4 points)

- The HMAC is a hash function, so it has the properties of the underlying hash too.
  • It is collision resistant
  • Given HMAC(K, M) and K, an attacker can't learn M - one way
  • If the underlying hash is secure, HMAC doesn't reveal M, but it is still deterministic
  • You can't verify a tag T if you don't have K
  • This means that an attacker can't brute-force the message M without knowing K

Q.16. How many key produced by HMAC? What are those keys? How to generate those keys? (4 points)

- Two keys are produced by HMAC to increase the security.
  • Output H[K+ opad) || H|K+ ipad) || M]]
  • If key is longer than the desired size, we can hash it first, but be careful with using keys that are too much smaller, they have to have enough randomness in them.
  Additional:
  • Use K to derive two different keys
  - • opad (outer pad) is the hard-coded byte 0x5c repeated until it's the same length as K+
  - • ipad (inner pad) is the hard-coded byte 0x36 repeated until it's the same length as K+
  - • As long as opad and ipad are different, you'll get two different keys
  - • For paranoia, the designers chose two very different bit patterns, even though they theoretically need only differ in one bit.

Q.17. What is authenticated encryption? Explain in detail two approaches in which authenticated encryption can be achieved. From the two approaches, which one is better? (4 points)

- Authenticated Encryption (AE) is a block cipher mode of operation which simultaneously provides confidentiality and authenticity (integrity) assurances on the data.

The two approaches in which authenticated encryption can be achieved are:
- Combine schemes that provide confidentiality with schemes that provide integrity
- Use a scheme that is designed to provide confidentiality and integrity
  - Method 1: Encrypt-then-MAC
    First compute Enc(K1, M)
    Then MAC the ciphertext: MAC(K2, Enc(K1, M))
  - Method 2: MAC-then-encrypt
    First compute MAC(K2, M)
    Then encrypt the message and the MAC together: Enc(k1, M || MAC(K2, M))
- Method 1 is better. Always use encrypt-then-MAC because it is more robust to mistakes.

Q.18. What are the characteristics of the output hash function (deterministic or non-deterministic)? Justify your answer. (4 points)

- A hashing function is a one-way function that takes some input and returns a deterministic output. The output is often referred to as a digest, a hash code, or simply a hash.

  The characteristics of the output hash function are:

  a. Deterministic - the same input always returns the same output. This is important because we need to know that we can trust the output of the function.
  b. Fast - they can be computed relatively quickly (although, in many applications, such as password hashing, slowness can be a desirable trait).
  c. One-way - it is infeasible to reproduce the input given the output. This maintains privacy of the original input, making it impossible to retrieve, for instance, and private key that was passed into the function.
  d. Unique - it is infeasible to find two inputs that produce the same output.

Q.19. What is a digital signature and describe its properties? (4 points)

- Digital Signature: The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation.

- Three parts:
  - KeyGen → PK, SK: Generate a public/private keypair, where PK is the verify (public) key, and SK is the signing (secret) key
  - Sign(SK, M) → sig: Sign the message M using the signing key SK to produce the signature sig
  - Verify(PK, M, sig) → {0, 1}: Verify the signature sig on message M using the verify key PK and output 1 if valid and 0 if invalid
- Properties:
  - Correctness: Verification should be successful for a signature generated over any message
    Verify PK, M, Sign(SK, M) = 1 for all PK, SK - KeyGen and M
- Efficiency: Signing/verifying should be fast

- • Security: Same as for MACs except that the attacker also receives PK

Q.20. Describe the steps of RSA digital signature algorithm? prove correctness of RSA digital signature. (4 points)

- The steps of RSA digital signature algorithm are:

  Step l:
  Generate a hash value, or message digest, mHash from the message M to be signed.
  Step2:
  Pad mHash with a constant value padding and pseudorandom value salt to form M'
  Step3:
  Generate hash value H from M'
  Step4:
  Generate a block DB consisting of a constant value padding 2 and salt
  Step5:
  Use the mask generating function MGF, which produces a randomized out-put from input H of the same length as DB
  Step 6:
  Create the encoded message (EM) block by padding H with the hexadecimal constant be and the XOR of DB and output of MGF
  Step 7:
  Encrypt EM with RSA using the signer's private key

  To check RSA’s correctness using Euler’s theorem:

  Theorem: sig^{e} = H(M) mod N
  Proof:
  sige = [HM)^{d}]^{e} mod N = H(M)^{ed} mod N
  = H(M)$^{k\Phi\ (n)+1}$ mod N
  = [HM)$^{\Phi(n)}$]^{k} • H(M) mod N
  = H(M) mod N

Q.21. What method has been used to guarantee RSA Digital Signature? (4 points)

- Necessary hardness assumptions:
  - • Factoring hardness assumption: Given n large, it is hard to find primes pq = n
  - • Discrete logarithm hardness assumption: Given n large, hash, and hash^d mod n, it is hard to find d

  • Salt also adds security
  • Even the same message and private key will get different signatures.

Q.22. What are the issues with public key encryption? Because of the issue what method we used to encrypt large size data that will be transmitted. (4 points)

- • Issues with public-key encryption
  - • Notice: We can only encrypt small messages because of the modulo operator

    - Notice: There is a lot of math, and computers are slow at math
    - Result: We don't use asymmetric for large messages
- Hybrid encryption: Encrypt data under a randomly generated key K using symmetric encryption, and encrypt K using asymmetric encryption
    - Enc_{Asym} (PK, K); Enc_{Sym}(K, large message)
    - Benefit: Now we can encrypt large amounts of data quickly using symmetric encryption, and we still have the security of asymmetric encryption

Q.23. Short answer Questions (12 points)

1. Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using a public key and a private key.
2. Asymmetric encryption transform plaintext to ciphertext using public key.
3. Asymmetric cryptography transforms plaintext into signature using private key.
4. Public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key.
5. RSA is an example of homomorphic encryption.
6. The SHA3 hash function is not vulnerable to length extension attack.