Chapter 07: Introduction to Cryptography

I. Overview

1. Cryptology
2. Security Services, Cryptography Primitives
3. Crypto-Systems (Symmetric, Asymmetric)
4. Two basic principles in cryptography algorithms
5. Stream cipher vs Block cipher
6. Approaches attacking a cipher (cryptanalysis, brute force)

II. Traditional Ciphers

1. Substitution Ciphers
   + Mono-alphabetic
   + Poly-alphabetic
2. Transposition cipher

III. Message Integrity & Hash function

1. Cryptographic Hash
   + Message Digest
   + Cryptographic Hash:
     - Properties: (compression, computational efficiency, random, avalanche effect)
     - Requirements (one-way, weak collision resistance, collision resistance)
2. Hash Algorithms:
3. Popular hash functions
   + MD5
   + SHA-1

IV Message Authentication Code (MAC)

1. Properties (arbitrary input length, fix output length, message authentication, integrity)
2. Limitations
3. HMAC

V. Digital signature

Questions

1. What are security services that cryptography provided?
2. What are cryptography primitives?
3. What are the essential ingredients of a symmetric cipher?
4. What are the two basic functions used in encryption algorithms?
5. How many keys are required for two people to communicate via a symmetric cipher?
6. What is the difference between a block cipher and a stream cipher?
7. What are the two general approaches to attacking a cipher?
8. Draft the block diagram of a Public-key encryption system.
9. Draft the block diagram of a Cipher-system using Digital signature.

10. In term of security services provided, is it safe to use a Cryptosystem with MAC + Encryption to transmit & receive message? Justify your reason.
11. Hashing is used to secure password in Linux. Alice and Bob unintentionally set their passwords similar. Are the stored password of both identical? Explain your answer.
12. Birthday attack and the application in cryptography
13. Why do SHA-2 hash functions use 224, 256, 384, and 512 as output bit length?
14. A plaintext message of 64 bytes is sending. To protect the message integrity, a SHA-256 message digest has been generated. Calculate the number of padding input bit for the SHA generator.
15. To verify the integrity of a 1KB plaintext, a MD5 digest is generated. How many bits are needed to pad to the plaintext?
16. Which security services does digital signature provide? Explain your answer.
17. Which cryptography primitives used in IPsec?

Chapter 08: Symmetric-Key Encryption

I. Modern Block Cipher
   1. Components (P-box, S-box, XOR operation, swapping, splitting, shifting, combining)
   2. Principles (confusion, diffusion)

II. Data Encryption Standard (DES)
   1. Feistel structure
   2. DES
   3. 3DES

III. Advanced Encryption Standard (AES)

IV. Encrypting large message
   1. Modes: ECB, CBC, CFB, OFB, CTR
   2. Evaluation criteria (Identical messages, Chaining dependency, Error propagation, Efficiency)

Questions

1. What are basic components of modern block cipher?
2. List various types of P-box that you know.
3. List properties of DES (bit size of input, output, and key)
4. Briefly describe functional blocks of Feistel structure, including input/output/key bit size.
5. Briefly describe functional blocks of DES cipher, including input/output/key bit size.
6. Briefly describe functional blocks of AES cipher, including input/output/key bit size.
7. How many versions of key in 3DES are there?
8. How many versions of AES are there? Describe the corresponding changes in internal structure of AES for each version?
9. What is the output of the first round of the DES algorithm when the plaintext and the key are both all zeros?
10. What is the output of the first round of the DES algorithm when the plaintext and the key are both all ones?

Chapter 09: Public-Key Encryption

I. Modular Arithmetic

1. Modulo, modulus
2. Congruence modulo
3. Properties (addition, subtraction, multiplication, exponentiation)
4. Modular inverse
5. Totient (Euler's phi) function

II. RSA
1. Algorithm
2. Encryption & Decryption
3. Example

III. Diffie-Hellman Key exchange
1. Algorithm
2. Example

Questions

1. Compute without a calculator.
   a) 15x29 mod 13
   b) 2x29 mod 13
   c) 2x3 mod 13
   d) −11x3 mod 13
2. Compute without using a calculator:
   a) $x=3^2 \bmod 13$
   b) $x=7^2 \bmod 13$
   c) $x=3^{10} \bmod 13$
   d) $x=7^{100} \bmod 13$
   e) $7^x = 11 \bmod 13$
3. Find all integers n between $0 \leq n < m$ that are relatively prime to m for $m = 4, 5, 9, 26$ (Euler's phi function)
4. Describe the RSA algorithm, including the encrypting & decrypting steps.
5. Let the two primes $p = 41$ and $q = 17$ be given as set-up parameters for RSA.
   a) Which of the parameters $e_1 = 32$, $e_2 = 49$ is a valid RSA exponent? Justify your choice.
   b) Compute the corresponding private key $K_{pr} = (p,q,d)$. Use the extended Euclidean algorithm for the inversion and explain every calculation step.
6. Encrypt and decrypt by means of the RSA algorithm with the following system parameters:
   a) $p = 3$, $q = 11$, $d = 7$, $x = 5$
   b) $p=5$, $q=11$, $e=3$, $x=9$
7. Why the Certificate Authority (CA) is needed in a public-key cryptosystem?
8. Which techniques behind a secured web transaction over the internet? Justify your answer
9. Describe the authentication based on public-key.
10. Https secures the transmitted data using the session key. How does this key being protected against the attackers.

11. Describe the security services embedded in credit card and the procedure that the card reader verifies the card in a particular transaction.
12. In RSA, given n = 12091, e = 13, and d = 3653 encrypt the message “THIS IS TOUGH” using the 00 to 26 encoding scheme. Decrypt the ciphertext to find the original message. Use 4-digit plaintext or ciphertext blocks.
13. In RSA, e is selected to be relatively prime to Phi(n). What would happened, if this condition is not met?