網路安全期中考題庫練習 2016-10-28

1. What is the zero-day vulnerability?

「Zero Day」是一個遠端程式碼執行漏洞。「該漏洞會使記憶體崩潰，並讓攻擊者能在使用者

當前使用的 IE 瀏覽器中執行任意程式碼。」



1. What is the “Watering Hole” attack?

「Watering Hole（水坑）」是用來描述針對性惡意軟體攻擊時，攻擊者入侵合法網站去插入一個「drive-by（偷渡式）」漏洞攻擊碼以攻擊網站訪客的流行用語。利用「drive-by（偷渡式）」漏洞攻擊碼是為了能夠不分對象地攻擊入侵越多的電腦

1. Explain the main functions of MAC address, IP address, and Port number in data transmission.
2. What is TCP three-way handshake protocol?
3. What is the TCP SYN flooding attack?

大量傳送SYN使對方消耗大量資源等待，進而造成其他正常使用者無法連線。

1. What is the ARP protocol? What is ARP spoofing?

used to convert an IP address to a physical address such as an Ethernet address.

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network.

1. What is the main function of DNS? What is DNS spoofing?

DNS: Domain Name System

DNS function: transfers URL to IP address

DNS spoofing is based on presenting fake DNS information to a victim in response to their DNS request and, as a result, forcing them to visit a site which is not the real one.

1. What are the six principles of security? Explain them.
2. Confidentiality
   1. Also called as *privacy*
   2. Refers to the secrecy of information
   3. Only the sender and the receiver should have an access to the information
3. Authentication
   1. Identifies the sender/receiver of a message
   2. Required so that the communicating parties trust each other
   3. Answers *who is who*
4. Integrity
   1. Ensures that any changes to a message are detected
   2. The message from the sender to the receiver must travel without any alterations
   3. Changes need to be prevented, or at least, detected
5. Non-repudiation

A user sends a message, and later on refuses that he had sent that message.

1. Access control

Access control specifies and controls who can access what.

1. Availability
   1. Resources/applications must be available to authentic users all the time
   2. Attackers can deny the availability
   3. *Denial Of Service (DOS)* is an example of an attack on availability
2. Please use a mathematical formula to describe the operation in round of DES.

Operation in one round

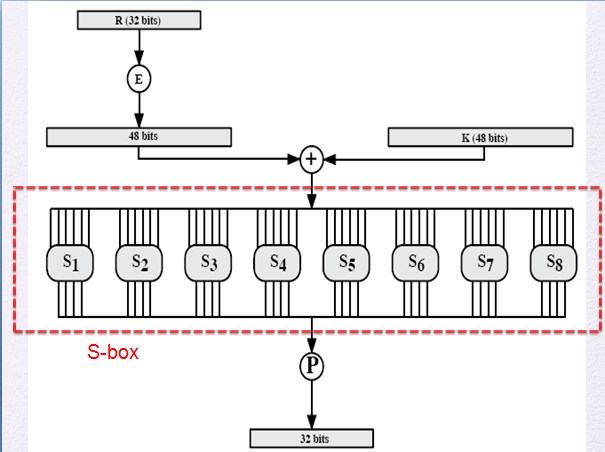
Li = Ri-1

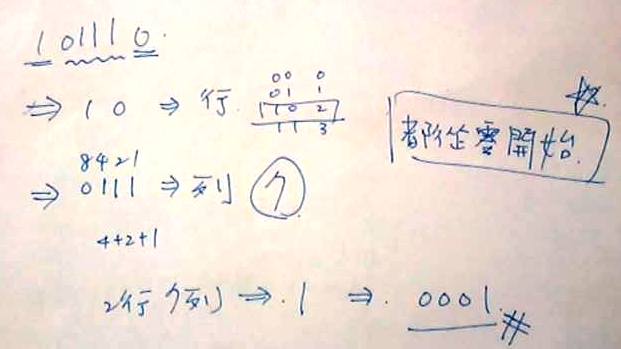
Ri = Li-1 ⊕ F(Ri-1, Ki)

1. (a) What is the function of S-box in DES algorithm?

(b) Given S2 below, what is the output regarding input as 001101.

(a)DES演算法核心:縮小位數輸入6bits輸出4bits，非線性置換



(b) 

1. Please show how to perform triple DES with two keys? How to perform triple DES with three keys?

C = EK1(DK2(EK1(P)))

C = EK3(DK2(EK1(P)))

1. What are the differences between ECB mode and CBC mode in DES? Why DES CBC mode is more secure than ECB?

stream ciphers串流加密 =>及時性加密，比較連續性封包，速度快且程式碼更少  
對明文一個位元一個位元地加密，就好像是明文不斷的流動進入加密器中加密，加密快速，因此能夠做到及時(real time response)的效果，適合用在語音傳輸加密中  
block ciphers區塊加密 => 相同狀態傳訊息封包，固定長度是可以分解成塊

是把明文切成固定大小的區塊，並用相同的密碼演算法和密鑰對每組分別進行加密和解密。由於要收集一定的資料量才可以做加密的動作，因此比較適合用來做檔案的加密

* 架構的金鑰是虛擬亂數位元產生器的輸入，並產生一連串看似隨機的8位元數字
* 金鑰串流應該儘可能接近真正的亂數串流
* 為了防止暴力攻擊，輸入密鑰需要足夠長;至少128位是可取的。

如果金鑰長度差不多相等，設計得宜的虛擬亂數產生器能讓串流加密法和區塊加密法一樣安全

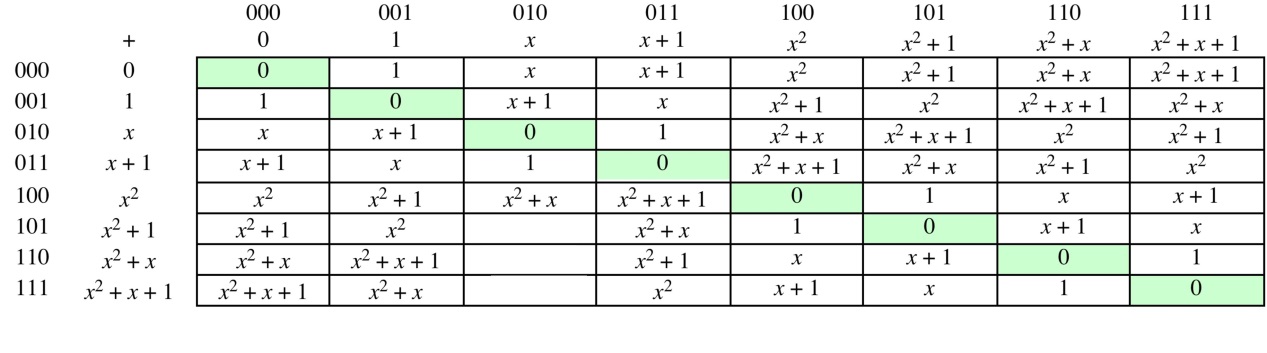
1. What is the avalanche effect while talking about DES/AES?

AES is stronger than that for DES (Table 3.2),

which requires three rounds to reach a point at which approximately half the bits

are changed, both for a bit change in the plaintext and a bit change in the key.

1. What are the differences between block ciphers and stream ciphers? Please list the four considerations on the design of stream ciphers.
2. Is the polynomial f(x) = x4 + 1 over GF(2) reducible? Prove or disprove.
3. With modulo *x*3 + *x* + 1, please fill in the three blanks in the following table.



1. There are four steps in one round of AES, including Substitute byte, Shift rows, Mix columns, and Add round key. Briefly explain them.
2. In AES (Advanced Encryption Standard) with mod *m*(*x*) = *x*8 + *x*4 + *x*3 + *x* + 1, what is the result of {03}•{6E}?
3. Explain the basic difference between HTTP and HTTPS. What is the basic function of digital certificates?
4. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 23 and a primitive root α= 5.

(a) If Bob has a public key YB = 10, what is Bob’s private key XB?

(b) If Alice has a public key YA = 8, what is the shared key K with B?

1. (a) Show that 5 is a primitive root of 23.

(b) Why do we need to select a primitive root to serve as α in the Diffie-Hellman algorithm?

1. Man-in-the-Middle attack could happen in the Diffie-Hellman key exchange protocol. Let the system parameters q = 11 and α= 7. Suppose the private keys of Alice (sender), Bob (receiver), and Darth (attacker) are 3, 9, and 6, respectively.

(a) What is the shared key between Alice and Darth? What is the shared key between Darth and Bob?

(b) How to achieve the Man-in-the-Middle attack in this case?

1. How to launch DOS(denial of service)/clogging attacks on the Diffie-Hellman key exchange protocol? Why?
2. Use Modular Arithmetic to compute 9103 mod 7.
3. Find the multiplicative inverse of 229 mod 31.
4. Describe how to generate the pair of public key and private key in RSA algorithm? (10%)
5. Let p = 7, q = 11, e = 13, and M = 5 (M: message). Show the details of the following questions. (10%)

a. What is the private key d ?

b. How to perform RSA encryption and decryption on the message M?

1. In RSA algorithm, why do we need the constraint “M<n” where M is the message and n is the system parameter? (If we remove the constraint, what happens?)
2. Since RSA cannot be directly applied to a large message (in this case M>n), how does RSA work with DES to encrypt a very large message M??
3. What are the differences between applying RSA to encryption/decryption and digital signature?