CBCS SCHEME

15CS61

USN 1 C R 1 6 C S 1 0 5

Sixth Semester B.E. Degree Examination, June/July 2019

Cryptography, Network Security and Cyber Law

Time: 3 hrs. Max. Marks: 80

Note: *Answer any FIVE full questions, choosing ONE full question from each module.*

Module-1

1 a. Describe the types of Vulnerabilities to domain of security. **(04 Marks)**

b. List the guiding principles of security. **(04 Marks)**

c. Write the extended Euclidean algorithm, with an example. **(08 Marks)**

OR

2 a. Calculate the value of x using Chinese remainder theorem by given below data :
$N = 210$, $n_1 = 5$, $n_2 = 6$, $n_3 = 7$, $x_1 = 3$, $x_2 = 5$, $x_3 = 2$. **(05 Marks)**

b. Explain the Vigenere Cipher and the Hill Cipher techniques with illustration. **(06 Marks)**

c. With neat diagram, explain Fiestel structure. **(05 Marks)**

Module-2

3 a. Illustrate the RSA algorithm for encryption and decryption. **(08 Marks)**

b. Briefly explain the practical issues of RSA algorithm. **(04 Marks)**

c. List the properties of the cryptographic hash. **(04 Marks)**

OR

4 a. *Discuss the case study : SHA – 1.* **(08 Marks)**

b. Explain the Man – In – the Middle attack on Diffie – Hellman key exchange, with neat diagram. **(08 Marks)**

Module-3

5 a. Explain the different Public Key Infrastructure (PKI) architectures. **(08 Marks)**

b. Describe the Mutual authentication using a shared secret. **(08 Marks)**

OR

6 a. Explain the Kerberos message sequence with diagram. **(06 Marks)**

b. Describe the IP Sec protocols Authentication Header and Encapsulating Security Pay load in transport mode. **(05 Marks)**

c. Explain Secure Sockets Layer (SSL) hand shake protocol. **(05 Marks)**

Module-4

7 a. Explain the Authentication and Master Session Key exchange in 802.11i. **(05 Marks)**

b. List and explain the worm characteristics. **(05 Marks)**

c. Explain Firewall functionality and Proxy fire wall. **(06 Marks)**

OR

8 a. Write a note on Intrusion Detection System (IDS). **(05 Marks)**

b. Explain the types of Intrusion Detection System. **(05 Marks)**

c. Briefly explain the Technologies for Web Services. **(06 Marks)**

Module-5

9 a. Explain Digital Signature Certificates. **(10 Marks)**

b. Describe the duties of Subscribers. **(06 Marks)**

OR

10 a. List any eight functions of the Controller. **(08 Marks)**

b. Briefly explain Penalties and Adjudication in IT Act. **(08 Marks)**

* * * * *

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

1.a . Types of Vulnerabilities

Vulnerabilities

- Weakness in a procedure, protocol, h/w or s/w within an organization that has the potential to cause damage.
- Vulnerability classes:
- 1. Human Vulnerabilities
- Induced by human behavior or action
- eg. clicking a link may leads to phishing or cross site scripting attack, e-mail virus

- 2. Protocol Vulnerabilities
- Protocols in LAN such as TCP, IP, ARP can be easily attacked
- Pharming attacks: ARP protocol to get passwords from LAN, man in the middle attack, replay attack

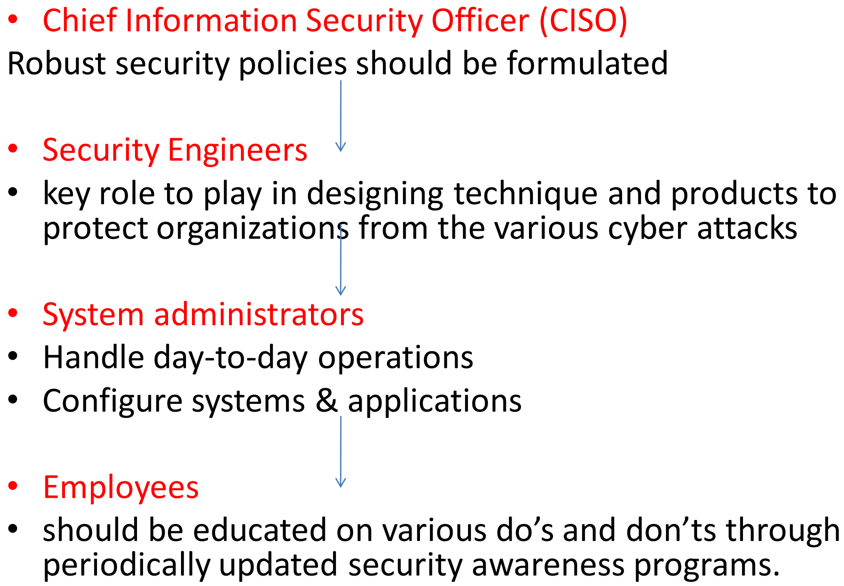
- 3. Software vulnerabilities
- In app’ s/w
- eg
- Without validation of limit of user input may lead to buffer overflow
- in text field if some java script is given then validation is stopped eg of cross site scripting vulnerability
- in text field if SQL query is given then validation is stopped eg SQL injection vulnerability

- 4. configuration vulnerability
- configuration settings in newly installed s/w can be given wrongly e.g read, write & execute privileges

B. Guiding principles of security

Guiding Principles

- 1. Security is as much a human pblm than a technological pblm & must be addressed at different levels
- It should be addressed by top level mgmt



- Chief Information Security Officer (CISO)

Robust security policies should be formulated

- Security Engineers
- key role to play in designing technique and products to protect organizations from the various cyber attacks

- System administrators
- Handle day-to-day operations
- Configure systems & applications

- Employees
- should be educated on various do’s and don’ts through periodically updated security awareness programs.

2. Security should be factored in at inception, not as an afterthought

- Application s/w is often vulnerable to attack
- Soln: Integrating secure coding practices into the s/w curriculum in the colleges
- 3. Security by obscurity- unknown(or by complexity) is often bogus- not genuine or true
- New security protocols may also have serious vulnerabilities
- They should be properly deployed in hacker perspective

4. Always consider the “Default Deny” policy for adoption in access control

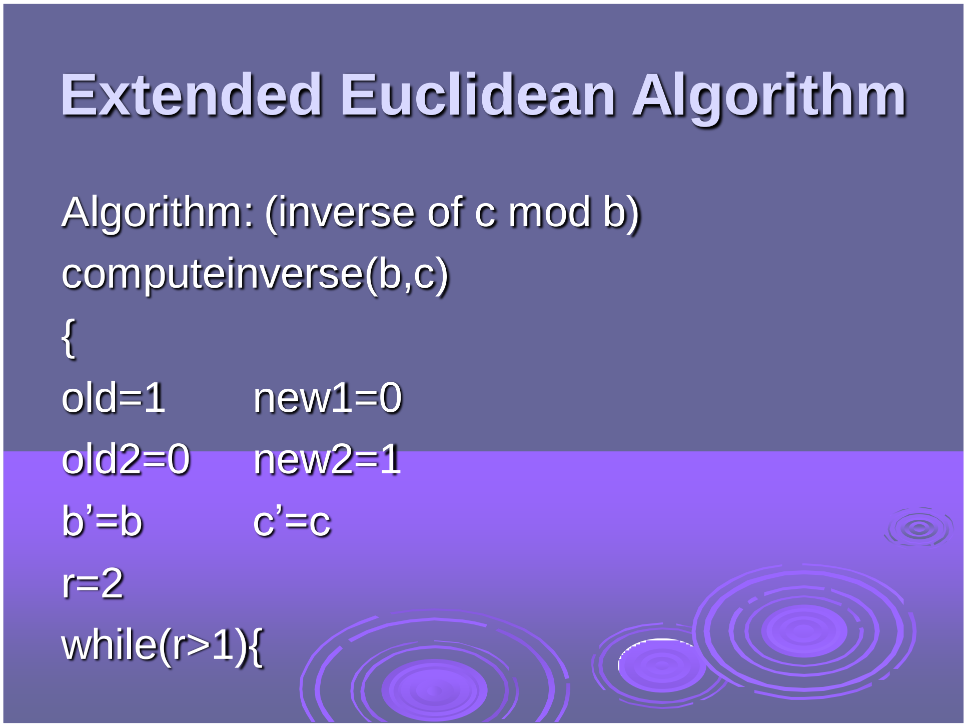
- Default Permit- unless subject(people, n/w packets.,,) is in Blacklist
- Default Deny – unless subject is in Whitelist
- Disadvantages:
- Mistakenly some legitimate subject whose name has been excluded from the whitelist
- Mistakenly some attacker subject whose name has been excluded from the blacklist

- 5. An entity should be given the least amount/level of permissions/privileges to accomplish a given task
- Role based access control: principle idea in RBAC is that mapping between roles and permissions
- 6. Use ‘Defense in depth’ to enhance security of an architectural design
- 2 firewalls configured by 2 different s/m administrators

7. Identify vulnerabilities & respond appropriately

- Risk assessment
- Risk=Assests X Vulnerabilities X Threat
- If the assests impacted by a vulnerability are of low value and /or the threat perception(probability that a vulnerabilty is successfully exploited) is small, then the associated is low.
- In such case it may not make economic sense to address such vulnerabilities

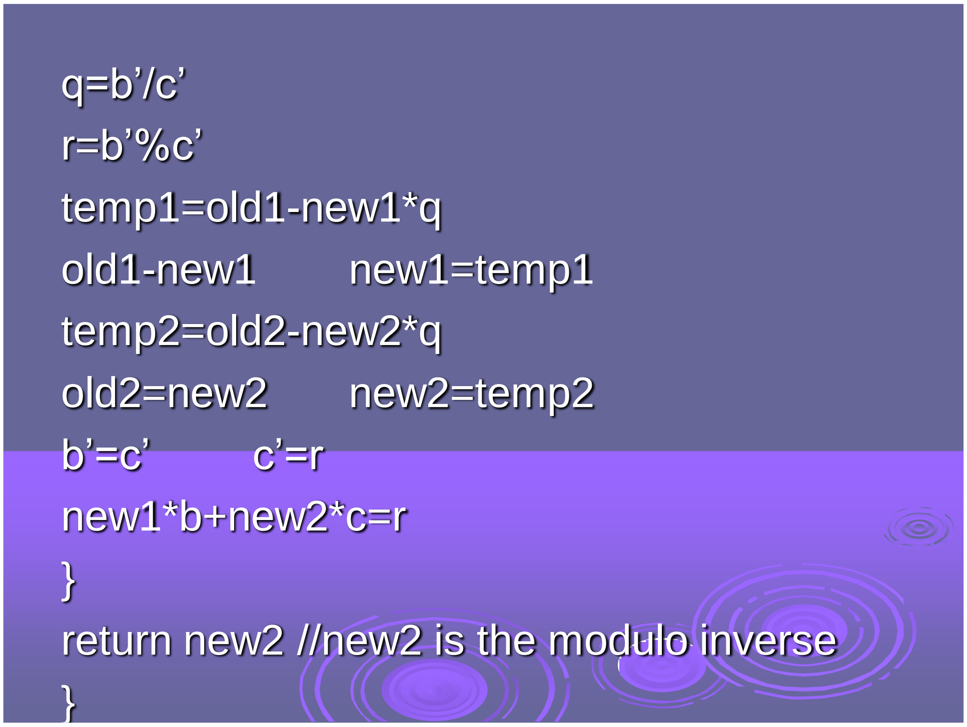
c. Extended Euclidean algorithm



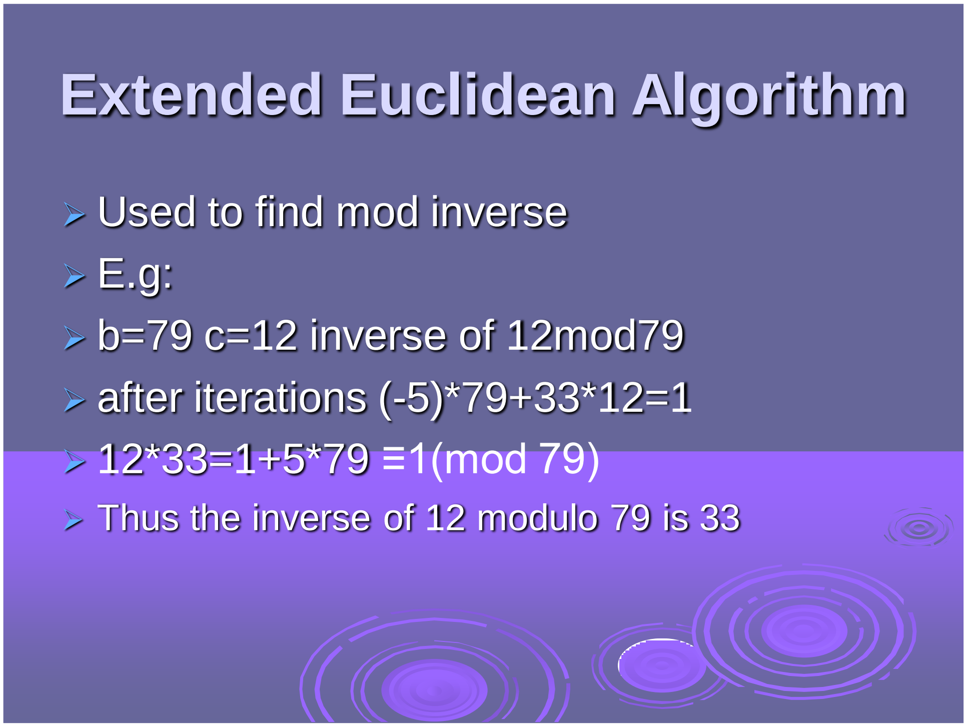
Extended Euclidean Algorithm

Algorithm: (inverse of c mod b)

```
computeinverse(b,c)
{
old=1       new1=0
old2=0      new2=1
b'=b        c'=c
r=2
while(r>1){
```



```
q=b'/c'
r=b'%c'
temp1=old1-new1*q
old1-new1        new1=temp1
temp2=old2-new2*q
old2=new2        new2=temp2
b'=c'       c'=r
new1*b+new2*c=r
}
return new2 //new2 is the modulo inverse
}
```



Extended Euclidean Algorithm

- Used to find mod inverse
- E.g:
- b=79 c=12 inverse of 12mod79
- after iterations (-5)*79+33*12=1
- 12*33=1+5*79 ≡1(mod 79)
- Thus the inverse of 12 modulo 79 is 33

2 Chinese Remainder Theorem

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

B Vignere Cipher and Hill Cipher

C. Feistel Cipher

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

2. a. RSA Algorithm

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

b. Issues In RSA.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

C. Properties of Hash function

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

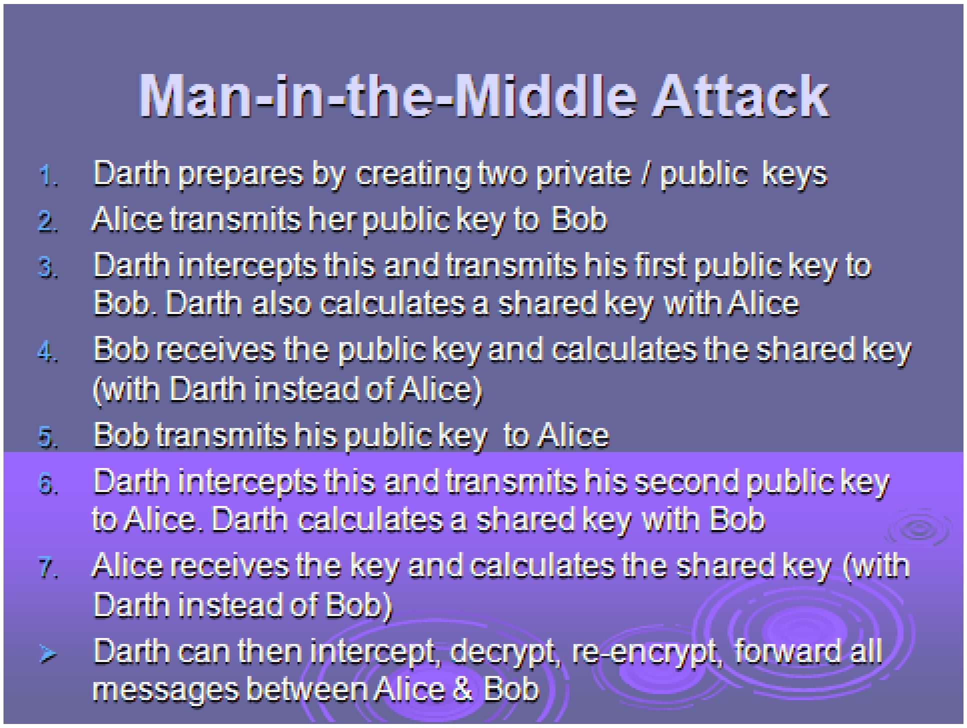
4. a. SHA-1Algorithm

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

b. Man-in the middle attack

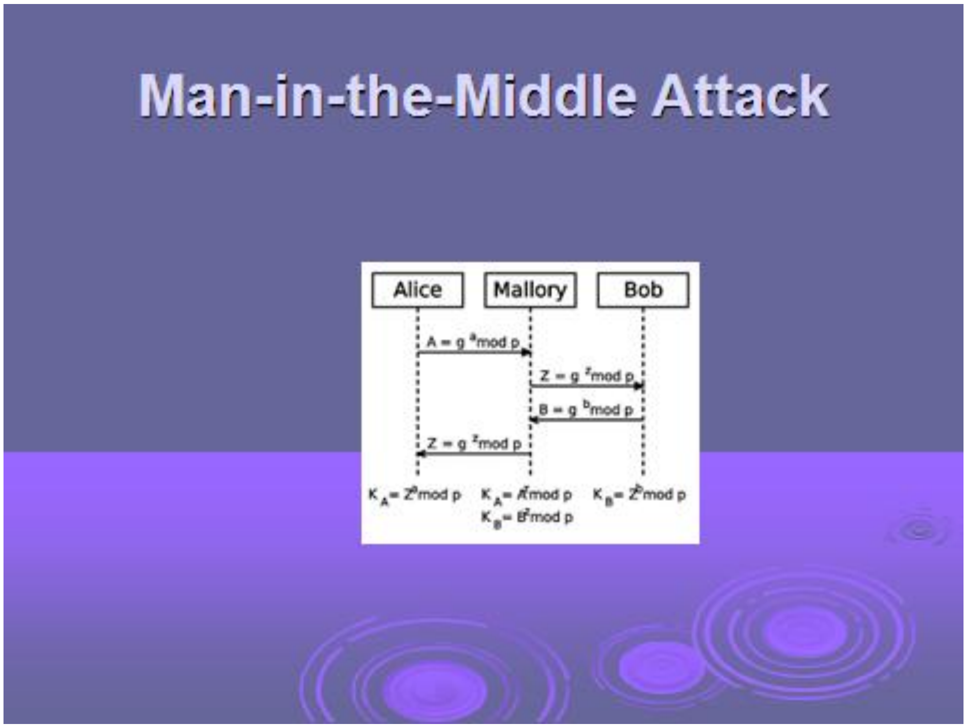


Man-in-the-Middle Attack

1. Darth prepares by creating two private / public keys
2. Alice transmits her public key to Bob
3. Darth intercepts this and transmits his first public key to Bob. Darth also calculates a shared key with Alice
4. Bob receives the public key and calculates the shared key (with Darth instead of Alice)
5. Bob transmits his public key to Alice
6. Darth intercepts this and transmits his second public key to Alice. Darth calculates a shared key with Bob
7. Alice receives the key and calculates the shared key (with Darth instead of Bob)

- Darth can then intercept, decrypt, re-encrypt, forward all messages between Alice & Bob

Man-in-the-Middle Attack


Alice
Mallory
Bob
$A = g^a \bmod p$
$Z = g^z \bmod p$
$B = g^b \bmod p$
$Z = g^z \bmod p$
$K_A = Z^a \bmod p$
$K_A = A^z \bmod p$
$K_B = B^z \bmod p$
$K_B = Z^b \bmod p$