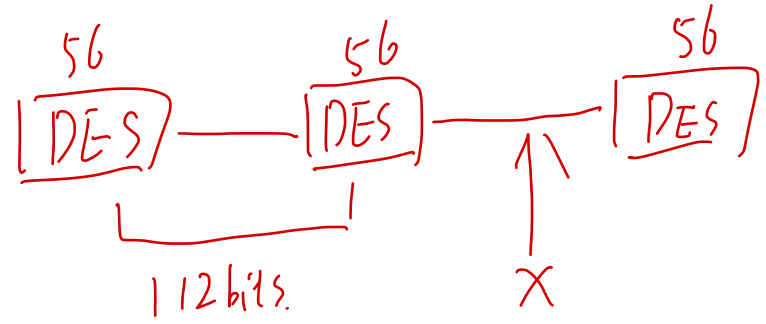
Name: _____ Student #: _____

ECE568 Assignment 2 (2019F)

Question 1: Block and Stream Ciphers [5 marks]

a. Why does 3DES (triple DES) only have an effective key length of 112 bits? (**2 marks**)

Because 3DES is vulnerable to the man in the middle attack.



b. What are the four rounds of AES encryption? Indicate what property (confusing and/or diffusion) each one provides (**1 mark**)

1. Byte sub – confusion
2. shift Rows – diffusion.
3. mix column – diffusion
4. Round key addition.

c. Fill in the encryption/decryption formula. (**2 marks**)

Mode	Encrypt	Decrypt
CBC	C1 = E(K, P1 + IV) Cj = E(K, Pj + Cj-1), j = 2, …, N	$P_1 = E(K^{-1}, C_1 \oplus IV)$ $P_j = E(K^{-1}, C_j \oplus C_{j-1})$ $j = 2, \cdots, N$.
CFB	$C_j = P_j \oplus E(C_{j-1}), j = 1, \cdots N.$	C0 = IV Pj = Cj + E(Cj-1), j=1,...,N

Name: _____ Student #: _____

Question 2: Cryptography [5 marks]

a. List 2 disadvantages of one-time pad. (**1 mark**)

1. The size of it needs to be as long as the message. (Could be too long)

Pick one [2. The one time pad needs to be sent in a completely secure channe

3. Can have the bits flipped

b. Indicate which of the confidentiality, integrity and authentication the following cryptographic mechanisms provide. (**2 marks**)

Mechanism	Confidentiality	Integrity	Authentication
RSA	✓		✓
SHA1	✓		✓
Diffie Hellman	✓	✓	
Digital Certificate + Public Key	✓	✓	✓

PICT

c. What value is used to prevent splicing attack? (**1 mark**)

Sequence #

d. List one advantage of using a MAC rather than a digital signature for authentication. (**1 mark**)

It's value produced is dependent on 1 sed

Name: _____ Student #: _____

Question 3: Web Exploits [5 marks]

a. Give an example of printing the web page's cookie to the screen. (**1 mark**)

Name: ....
Content: ....
Domain: xxx.com
Send For: Any type of connection
Expires: June-08-69 6:01:01 PM.

b. Order the steps that happen in SSL protocol. (**2 marks**)

1	Client and Server agree on a Cipher Suite	(1)
2	Client and Server compute master secret	(4)
3	Server sends its certificate	(2)
4	Client sends its certificate	(3)

c. Give 2 reasons why using authentication cookies is better than basic HTTP authentication. (**2 marks**)

1. Session Ids are being compared when sending cookies instead of raw username and passwords via basic Auth.
2. An expiration time is specified, where as for basic Auth it requires users to close the browser completely.

Name: _____ Student #: _____

Question 4: Miscellaneous [5 marks]

a. How is the origin of a script or data determined in web programming? (**1 mark**)

1. Protocols
2. Domain Name
3. Port #

b. Give 1 defense method against XSS and 1 method to protect cookie from being stolen. (**2 marks**)

Defense:
Convert all special characters before sending it to a user.

Method:
Use HTML_only cookies. That way no Javascript can access cookies.

c. Alice uses a cryptographic has to compute a hash of a message, which she sends to Bob over a secure channel. She then sends the message over an insecure channel. Bob uses the hash to verify that the message is correctly received. What property of cryptographic hashes are Bob and Alice utilizing here. (**1 mark**)

Integrity via the collision Resistance Property.

d. Select all cryptographic techniques that SSL uses? (**1 mark**)

Asymmetric-key cryptography	✓
Symmetric-key cryptography	✓ (double check)
Cookies	
Hash functions	✓
PKI certificates	✓