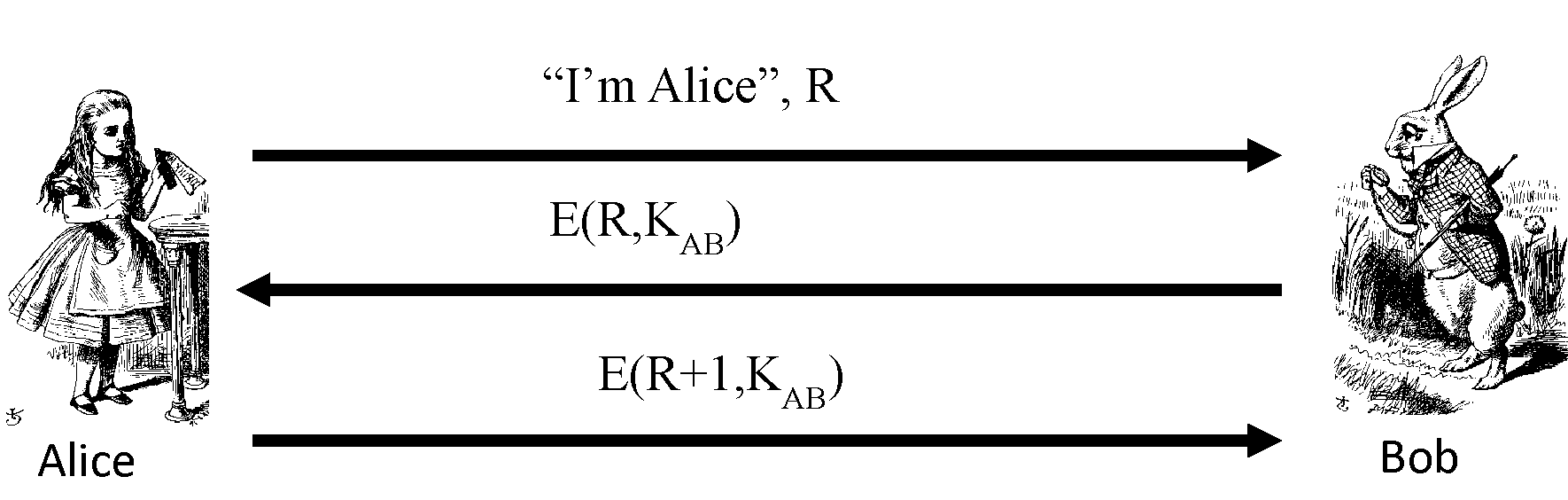
### Homework 3 Pramod kumar [pjk5502@psu.edu](mailto:pjk5502@psu.edu) 963884608

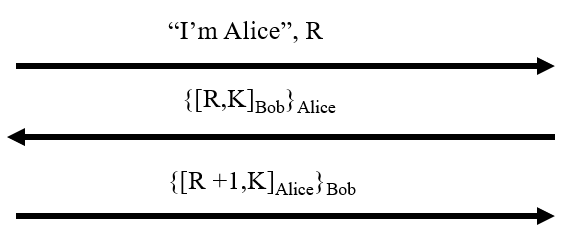
1. (10 pts) Consider the following mutual authentication protocol. Give two different attacks Trudy can convince Bob she is Alice.



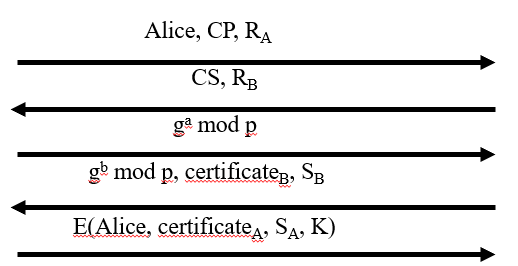
Answer :

1. Replay attack - Trudy can replay the messages sent by Alice to Bob and pretend to be Alice. As signature is not required, replay attack is possible.
2. Trudy sends a fake message to Bob saying “I am Alice” + R. Bob replies with E(R, K). Trudy doesn’t know K. But he knows R+1. So he sends another message with “I am Alice”, R+1. Bob replies with E(R+1, K). This is the reply to the first connection that Trudy made. Thus Trudy can convince Bob she is Alice.
3. (10 pts) Design a secure two-message authentication protocol that provides mutual-authentication and establishes a session key K. Assume that Alice and Bob know each other’s public keys beforehand.

since they both know each other's public keys, we can use them to encrypt messages so that only the owner can see those messages with private key.

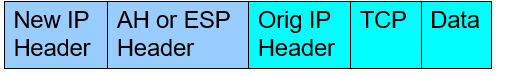
Alice  Bob

SSL another example for mutual authentication

Alice  bob

1. (10 pts) SSL and IPSec are both designed to provide security over the network.
2. What are the significant similarities between the two protocols?
3. What are the significant differences between the two protocols?
4. For SSL, what protocol does it use to establish security contexts (e.g., keys and algorithms) between two parties? How about IPSec?
5. What will a packet look like if you (IP address A) send a packet to another machine (IP address B) with AH at tunnel mode?

Answers :

1. Both provide- encryption, integrity protection, and authentication
2. Differences
   1. Both are on different layer of the protocol stack. ssl on socket layer and ipsec on network layer
   2. Ipsec is built in the OS while SSL doesnt need OS support.
   3. ipsec is more complex to implement while SSl is simple
   4. IPsec doesn't mandate any way to generate keys, select algorithms, or to establish contexts. Whereas SSL has has embedded in it an authentication and key establishment protocol.
   5. SSL is over reliable transport (usually TCP), IPsec is over unreliable transport
   6. IPSec is designed to protect IP traffic whereas SSL is designed to protect any byte stream
3. it uses digital certificate, Public key, or password for authentication. IPsec uses authentication headers and encapsulating security payload protocol.
4. Packet will have AH OR ESP header along with new and original ip header.

d.

1. (10 pts) Consider the Kerberized login discussed in this chapter.
2. What is a TGT and what is its purpose?
3. Why is the TGT sent to Alice instead of being stored on the KDC?
4. Why is the TGT encrypted with KKDC?
5. Why is the TGT encrypted with KA when it is sent from the KDC to Alice’s computer?

Answers :

1. TGT stands for ticket-granting ticket. This is time stamped and encrypted. This encrypted result is returned to Alice’s computer and is used to enable access to network resources.
2. 1) it help in maintaining statelessness 2) if TGT stored on server then for every next message transfer alice has to got to KDC to encrypt and similarly while receiving message too. which is not scalable option. KDC is just used to generate TGT befor getting in actual communication.
3. TGT contain information about sender too, which help in mutual authentication. since it is encrypted with KDC, alice or trudy cant decrypt it and bob can use to ask KDC for determining identity of callee.
4. Because only alice and KDC knows that key. Hence KDC encrypt with alice key so that trudy can't decrypt it.
5. (8pts) Describe (enumerate) the insecurity of GSM and then modify the GSM security protocol (Figure 10.25) so that it can provide mutual authentication.

Answer :

GSM security flaws -

* Crypto flaws - The hashes A3 and A8 are based on COMP128 hash function which violates Kerckhoffs’ principle. This has a record of being broken.
* Design flaws - GSM phone call is encrypted between the mobile and the base station but not from the base station to the base station controller.
* SIM attacks -
  + Optical fault induction : an attacker could force a SIM card to divulge its Ki by using an ordinary flashbulb.
  + Partitioning attacks : timing and power consumption analysis could be used to recover Ki using only eight adaptively chosen plaintexts
* Fake base station -
  + Authentication is not mutual
  + Encryption is not automatic
* No replay protection

Additional Questions:

5.17 (8pts):

1. Difficulty that 2 value match to same hash. The hash function "uniformly" distributes the data across the entire set of possible hash values.
2. Charlie knows the range of bid (10000 to 20000). From this, Charlie can compute all the 10000 possible hash values. When Alice and Bob place their bids, Charlie can match the hash value and know their exact bids. And later can put up a higher bid to win it.
3. Yes, as described in ans b, this is a security concern as the person who places the last bid clearly has an advantage over the other two.
4. To overcome forward search attack, we can append random bits to the hash. This way, Charlie cannot know the exact bid.

5.21 (6pts):

* Advantage of (i) - As the key is not stored in Alice’s computer and is generated every time when it is required, it is more secure. No one can get the key by hacking Alice’s computer
* Advantage of (ii) - since key here is not depended on hash value of password, hence key is secure from hashing attack. secondly, if someone get to know alice password, he wont be able to decryt the communication because he will need E(KA,K) from alice computer. which is kind of physical barrier.

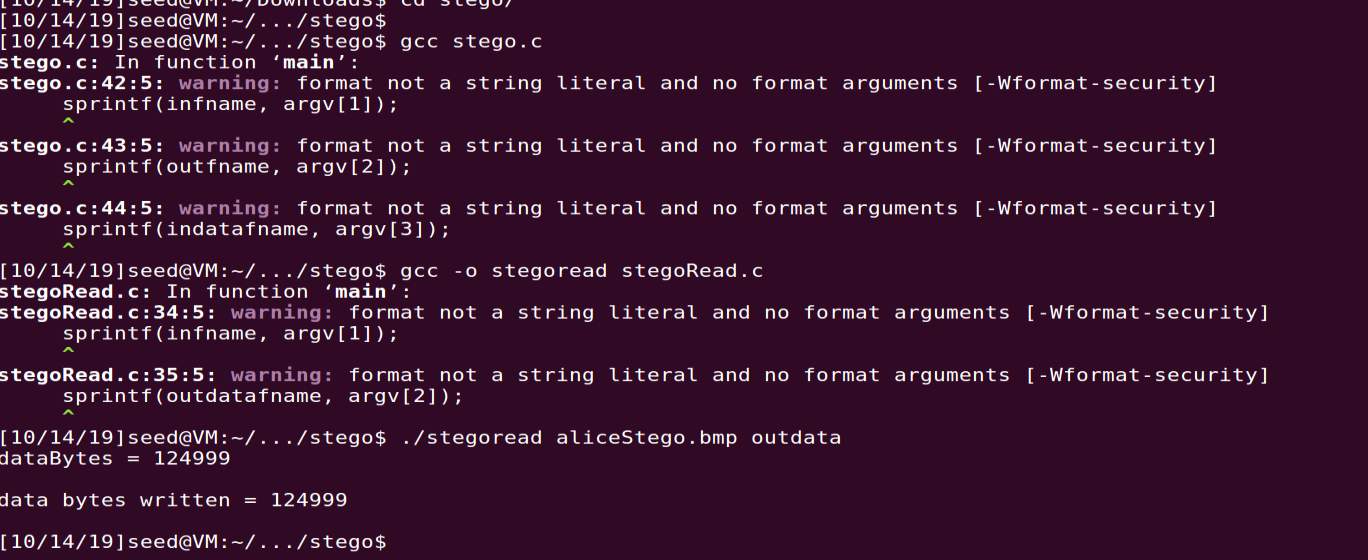
5.33: (6 pts, part a only)

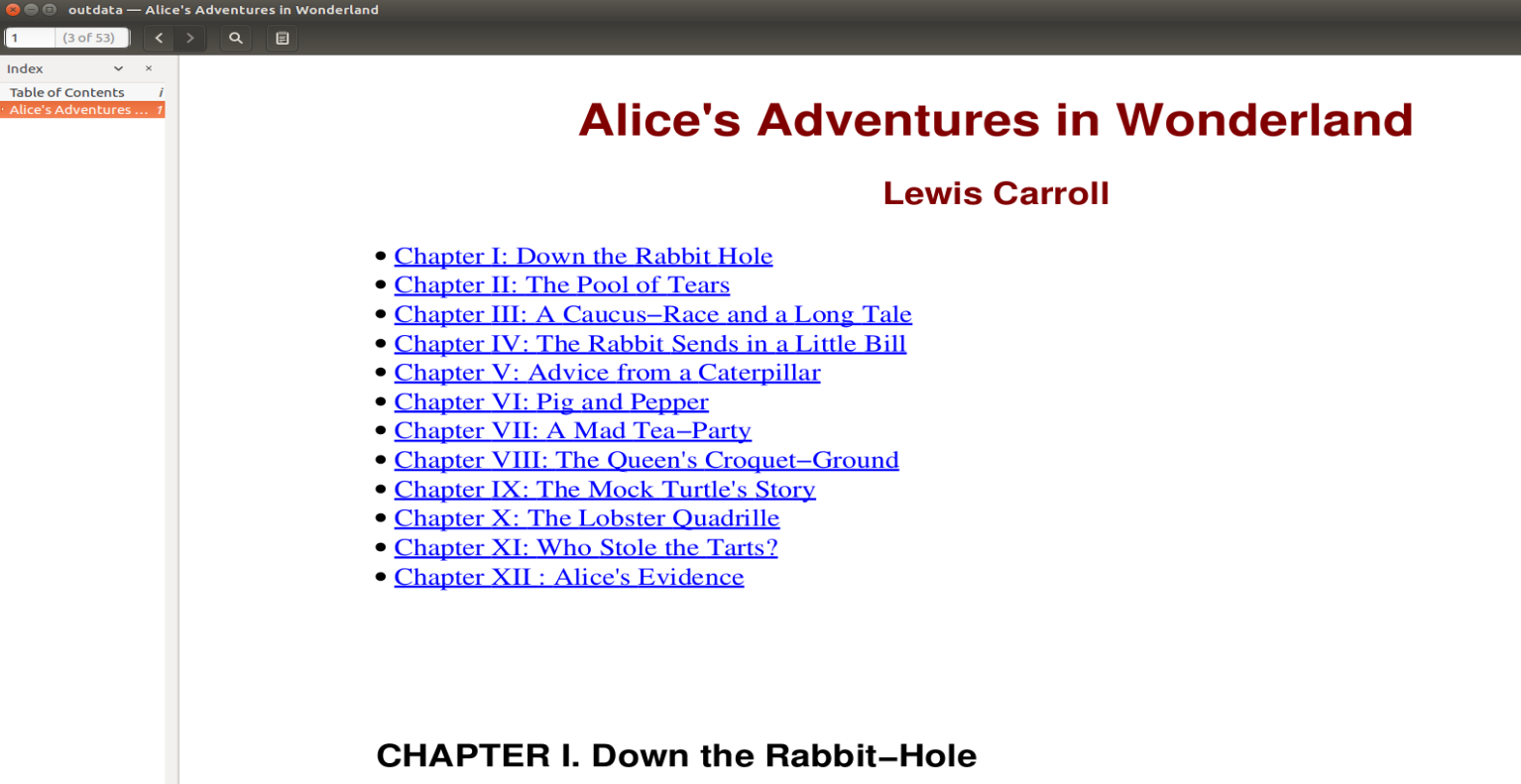
1. Equation of the line : y = -2/3x + 6

5.42: (10 pts, a, b 4 pts each, 2 pts for c)

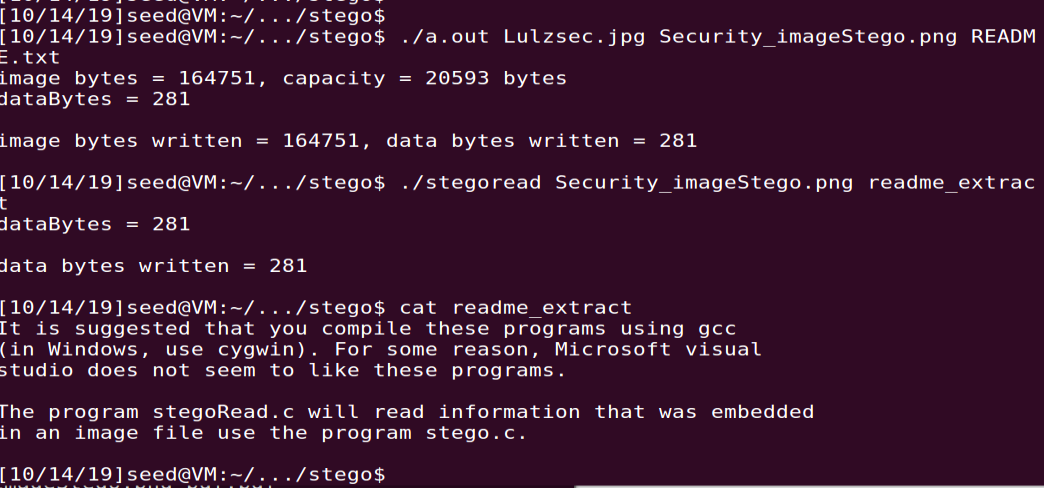
(<http://www.cs.sjsu.edu/~stamp/infosec/files/>)

part A

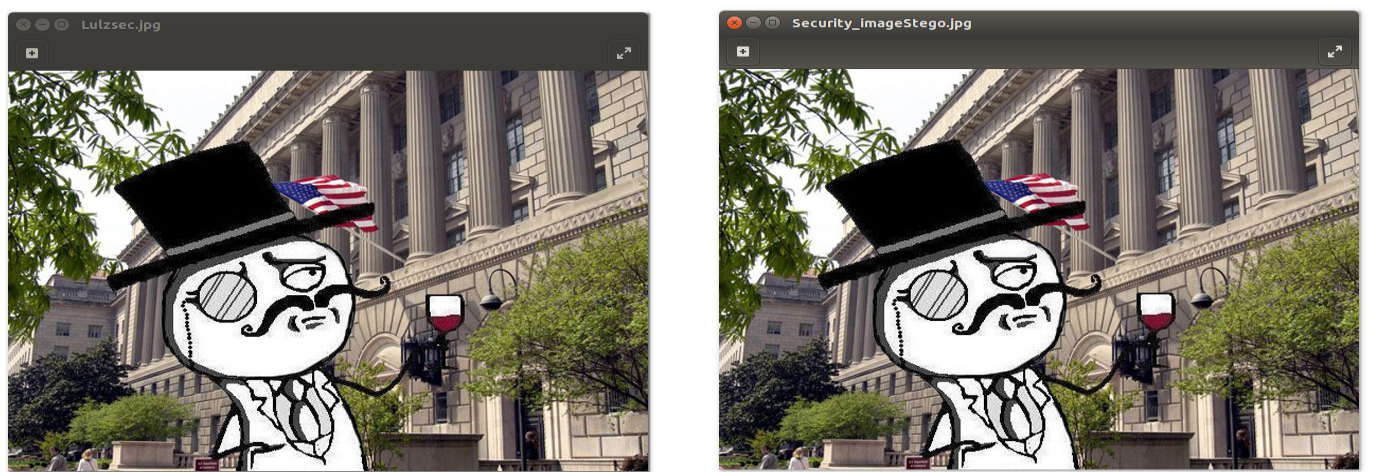




Part B:



part C:



5.48: (6 pts)

1. Random numbers are used which is called IV (initialization vector) to generate encrypted cipher text.
2. Random numbers are used to generate RSA key pairs (i.e., randomly selected large primes), and Diffie-Hellman secret exponents.

5.49: (8 pts)

1. Random numbers used in many non-security applications such as simulations only need to be statistically random, that is, they must be indistinguishable from random in some statistical sense. Whereas, cryptographic random numbers must be statistically random and must be unpredictable.
2. Yes, it is a practical security concern. Consider this example - Suppose a server generates symmetric keys for users as follows - Ka for Alice, Kb for Bob, Kc for Charlie and KD for Dave. According to the scenario given in the question, Alice, Bob and Charlie can get together and predict Kd. This proves that the system is compromised.

10.1. (8 pts)

1. Alice is authenticated at the last step when she sends an encrypted block having her identity, certificate and signed value. Nonce R\_A provides replay protection. Only Bob can send the correct response as a signature is required.
2. because it is encrypted with bob public key and can only be decrypted by bob.
3. Yes, trudy can impersonated the Bob, may get the key but alice wont be able to authenticate bob as it may not have valid CA certificate. that's the reason protocol doesnt break as authentication itself will fail and we may not proceed with the ssh connection.
4. since public/private key based encryption is computationally costly, they are just used to exchange the keys, once key is derived further communication will be done using symmetric key.