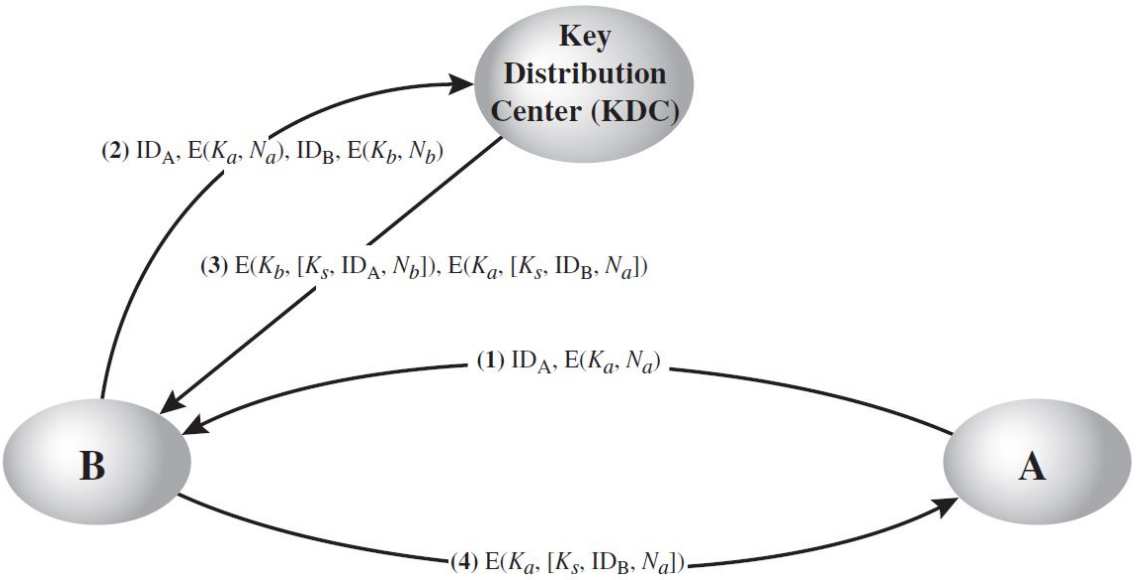
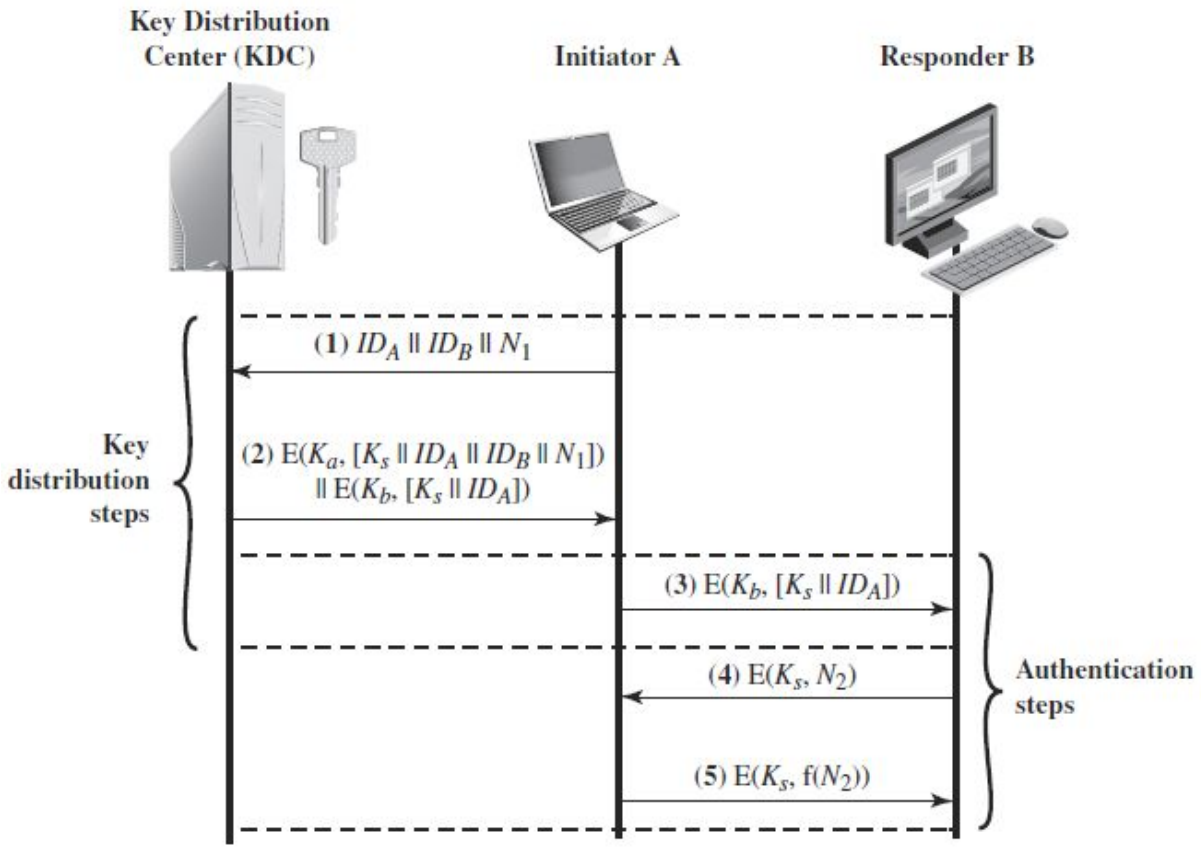
Vaibhav Sharma
200365101
Cs435- Assignment 3

1. (20 points) One local area network vendor provides a key distribution facility, as illustrated in the following Figure A3-1.
a. Describe the scheme.
b. Compare this scheme to that of Figure A3-2. What are the pros and cons?





Solution -

2. (12 points) Explain the problems with key management and how it affects symmetric cryptography.

Solution -

The problems with the key management is the vulnerability to man in the middle attack or a third party changing the message and make it look like the sender initially sent something else in case of losing the private secret key.

When adding key management in symmetric cryptography, one of the major concerns is the use of common private key. Due to the nature of symmetric cryptography, both sender and receiver use the common key to encrypt and decrypt which is a problem because it creates the need to transfer keys between each other vulnerable to attacks and thus can lead to a third party getting the key and data.

3. (6 points) What are two different uses of public-key cryptography related to key distribution?

Solution -
The two different uses of public-Key cryptography are ":

- Digital Signatures
- Asymmetric encryption

4. (6 points) List four general categories of schemes for the distribution of public keys.
Solution -
The four general Categories are

- Public Key certificates
- Public announcement
- Public authority
- Public available directory

5. (10 points)

Suppose H(m) is a collision-resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, x' with $x \neq x'$, we have $H(x) \neq H(x')$ Explain your answer.

Solution -
If H(m) is collision-resistant hash function that maps a message of arbitrary bit length into n-bit hash value then that implies that there a 2^n possible outputs of arbitrary input. This means. More than one input can have the same output. So it could be possible that x is not equal to x' but H(X) = H(X') hence, proving the statement false.

(6 points) What is the role of a compression function in a hash function?

Solution -
A compression function takes constant length input and returns a constant length output. It a date and breaks it into small blocks of certain length depending on the compression function and pad it in a way so the size of the message is a multiple of the block size. Then the blocks are hashed sequentially to create output.

7. (10 points) What types of attacks are addressed by message authentication?
Solution -
The type of attacks addressed by message authentication are:

- Sequence modification
- Timing modification
- Content modification

8. (6 points) What is the difference between a message authentication code and a one-way hash function?
Solution -

- Message authentication code uses a secret key to provide authentication whereas one way hash function uses secret key for hash function but does not provide authentication.

- Message authentication code uses the same secret key to encrypt and decrypt where as hash function uses public key to encrypt and private key to decrypt

9. What are the properties a digital signature should have?
Solution -
Digital signatures should have time, author and date. They should be verified by third parties and authenticate the content at the time of signature.

10. (10 points) What requirements should a digital signature scheme satisfy?
Solution -
Digital Signature scheme should deny creation of false signatures and multiple messages on the same signature. It should be easily verified and recognized and have a pattern with the message being signed.

11. (8 points) In what order should the signature function and the confidentiality function be applied to a message, and why?
Solution -
The signature function is applied before the confidentiality function. The reason behind following this order is to enable a third party to verify any disputes because if we apply the confidential function before the signature function then third party requires a decryption key to verify the message.