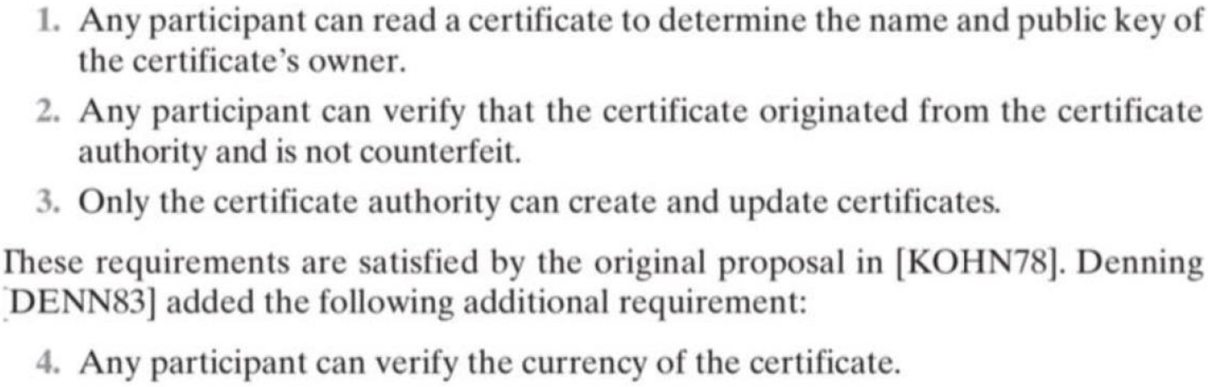
Compare between:

1. SSL connection and SSL session
2. Steganography and Encryption
3. Diffusion and Confusion
4. Block Cipher and Stream Cipher
5. Active and Passive attacks

State the requirements needed in any certificate issued by a certificate authority

Answer:



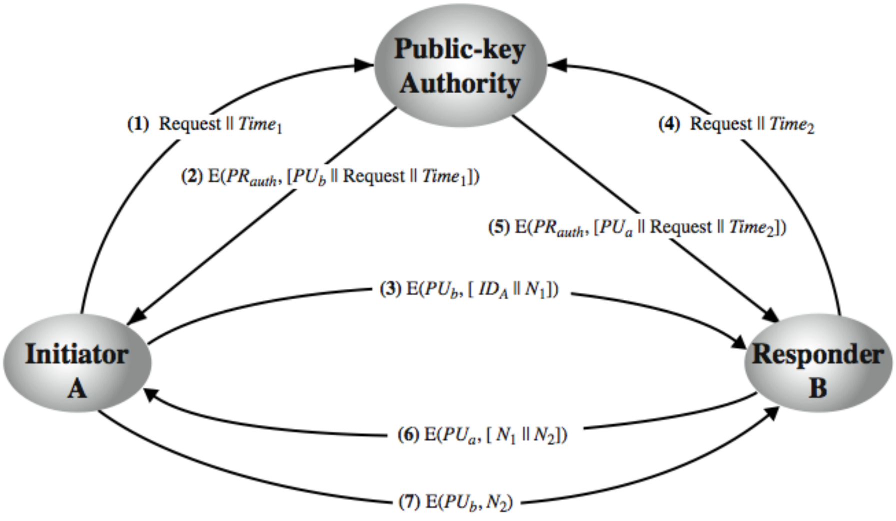
1. Any participant can read a certificate to determine the name and public key of the certificate's owner.
2. Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
3. Only the certificate authority can create and update certificates.

These requirements are satisfied by the original proposal in [KOHN78]. Denning [DENN83] added the following additional requirement:

4. Any participant can verify the currency of the certificate.

Assume you have a Public Key authority. Sketch the diagram showing your bla bla bla

Answer:


Public-key Authority
(1) Request || $Time_1$
(4) Request || $Time_2$
(2) E(PR_{auth}, [PU_b || Request || $Time_1$])
(5) E(PR_{auth}, [PU_a || Request || $Time_2$])
(3) E(PU_b, [ID_A || N_1])
Initiator A
Responder B
(6) E(PU_a, [N_1 || N_2])
(7) E(PU_b, N_2)

Sketch 1 round of DES

Answer:

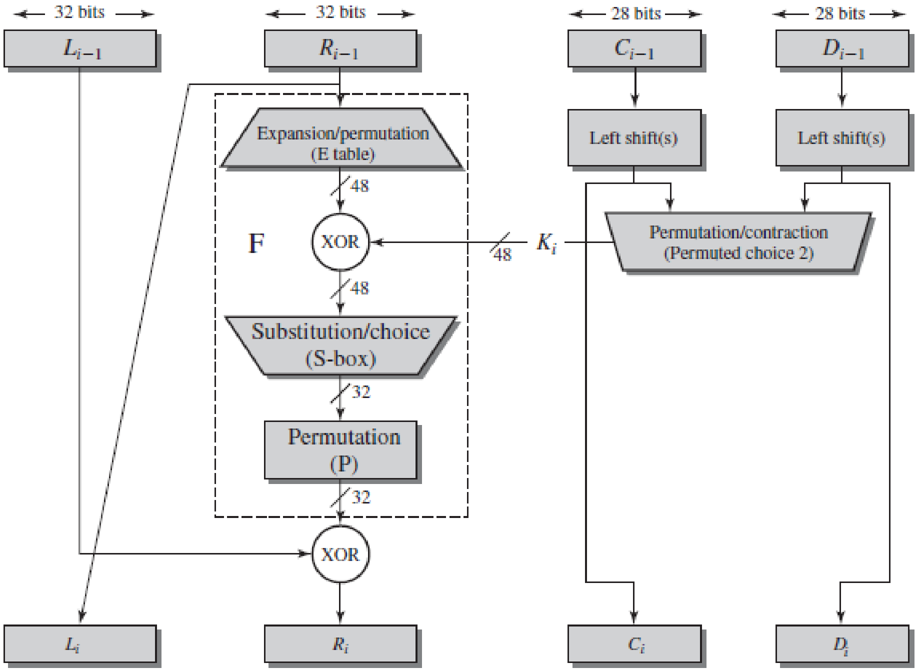
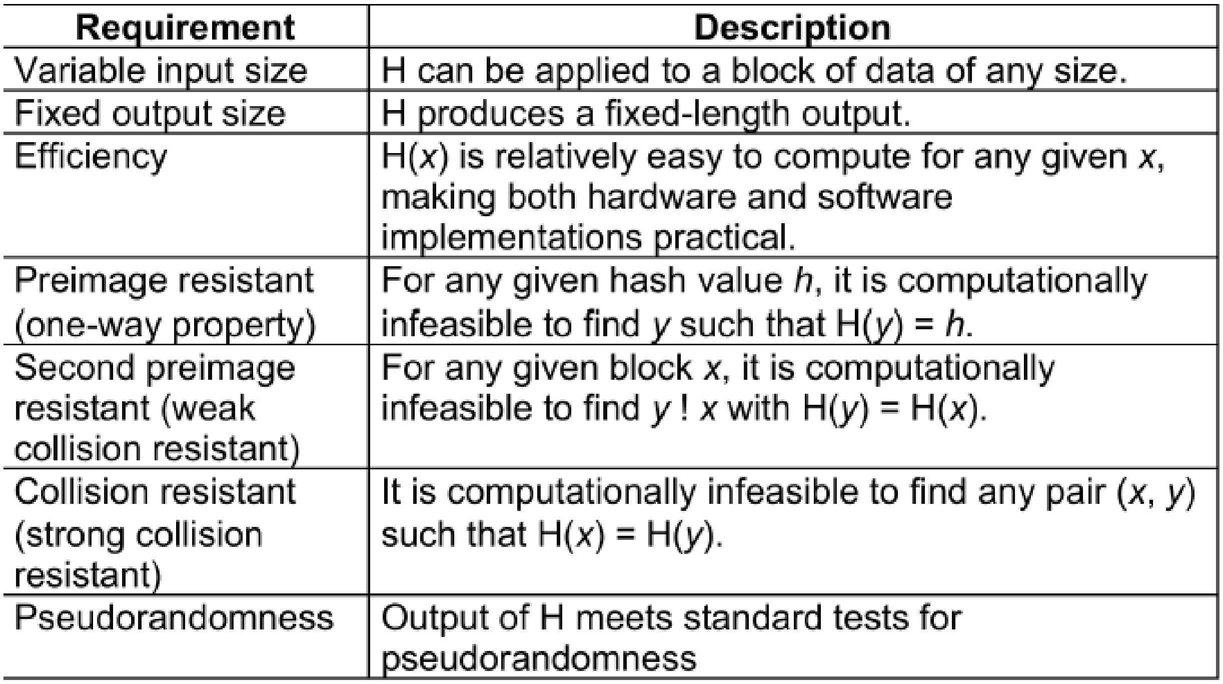


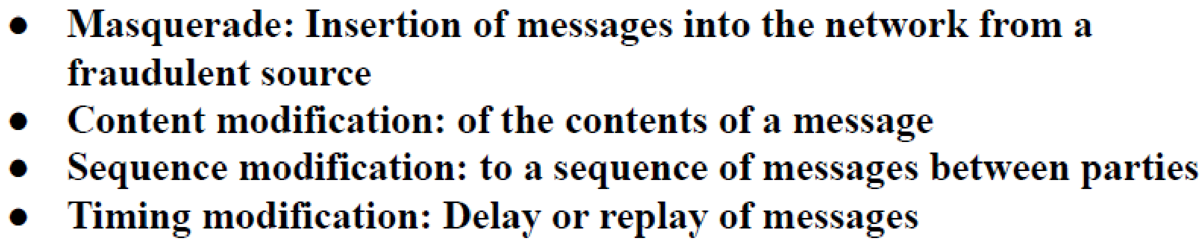
Figure 3.6 Single Round of DES Algorithm

What are the requirement of hash function?



Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	H(*x*) is relatively easy to compute for any given *x*, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value *h*, it is computationally infeasible to find *y* such that H(*y*) = *h*.
Second preimage resistant (weak collision resistant)	For any given block *x*, it is computationally infeasible to find *y* ! *x* with H(*y*) = H(*x*).
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (*x*, *y*) such that H(*x*) = H(*y*).
Pseudorandomness	Output of H meets standard tests for pseudorandomness

What types of attacks are addressed by message authentication
(State and describe briefly at least 3 attacks)?



- **Masquerade: Insertion of messages into the network from a fraudulent source**
- **Content modification: of the contents of a message**
- **Sequence modification: to a sequence of messages between parties**
- **Timing modification: Delay or replay of messages**

In block cipher operations, during the transmission of C3 (the third cipher block) an error in the 5th bit occurred. How many plaintext blocks will be affected, if we are using:

1. 16-bit CFB mode? Explain why?
2. 8-bit OFB mode? Explain Why?

Answer in mid 2019

1. Additive inverse of 15 mod 17
2. For a short message, which is best to use for encryption/decryption:
    a. OFB
    b. CBC
    c. CFB
    d. ECB
3. GCD of 1234 and 4321 (aw mult. Inverse m4 fkra)