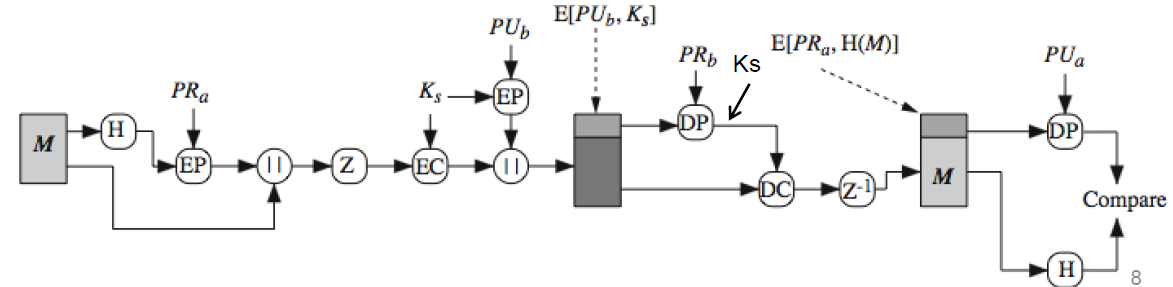
Answer the following questions related to the diagram below (PGP Operation)

1) Does the illustrated PGP operation provide confidentiality, or only authentication?

2) What is the role of the module Z?

3) Why is the session key Ks encrypted?

4) Does the destination first decrypt the message M, or decrypt the hash code first?



M - message, H - Hash, PR - private key, EP - Encryption, Z - compression, EC - session key

1) it provides both confidentiality before the compression and authentication after that by encrypting the session key with the public key.

2) Z is the compression part for saving on communication overhead.

3) for security, the session key needs to be encrypted to be shared between the sender and the recipient.

4) first the message is decrypted with the private key next we decompress and finally compare the hash with the public key

Name the four services provided by Pretty Good Privacy (PGP) for E-mail security

Authentication,

Confidentiality,

Compression,

E-mail compatibility

Which of the following statements are true? Explain briefly.

a) A hash function H takes a message M as input and produces a fixed-length output h=H(M)

b) The hash function should be easy to compute for any message M

c) The inverse of the hash function should be easy to compute, i.e. given the output h, it should be feasible to find M subject to H(M)=h

d) It should be feasible to find two different messages M1 and M2, for which H(M1)=H(M2)

a) is true

b) true

c) it should not be easy to inverse the hash function it is almost mathematically impossible to find the inverse of a hash with the output

d) it should not be able to find two messages with the same hash.

One of the main differences between a Hash function and a MAC is that a hash function maps the message into a fixed-length hash value which serves as the authenticator, while MAC takes as input both the message and a secret key and outputs a fixed-length value that serves as the authenticator.

True

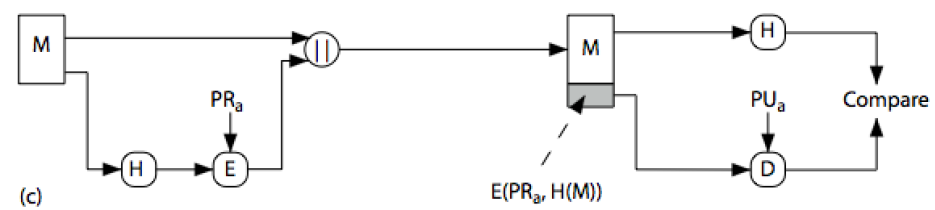
SSL is most widely used Web security mechanism  
SSL is designed to make use of TCP to provide a reliable end-to-end secure service  
Subsequently became Internet standard known as Transport Layer Security (TLS)   
SSL is not a single protocol, SSL has two layers of protocols (next slide)

True

When Web Security is provided on the transport layers (as in e.g. TLS), it is tailored to the specific needs of a given application

False

The diagram below illustrates a method to provide digital signature with Hash Functions



Which of the following statements are true? Please explain.

a) The destination needs to know the sender's private key in order to verify the integrity of the message

b) An attacker can alter the message if it knows the sender's public key

c) Digital signature is provided because the hash value of the message M is encrypted with a private key

d) Confidentiality of the message M is provided because the hash value of the message M is encrypted with a private key

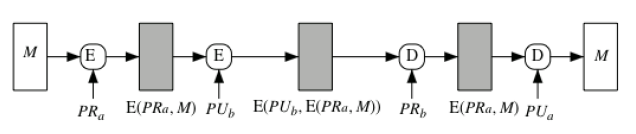
 a) is not true because it doesn't need the private key it only needs the public key to compare with the hash.

b) not true because everyone has the sender's public key it can only verify with the public key not alter the message

c) is true

d) is not true because the message itself is not encrypted.

What does the illustrated block diagram represent? Describe in detail



This scheme provides authentication and confidentiality first, we have the message then a private key of the authenticated user then we encrypt the message with the private key. then we use both the private and public key and encrypt the message again. To decrepit the message we need to use both the private and public key.

SSL Handshake  protocol It is  the most complex part of SSL,  it allows server & client to:

– Authenticate each other

– To negotiate encryption & MAC algorithms

– To negotiate cryptographic keys to be used

 Handshake Protocol is used before any application data is transmitted

 Handshake Protocol consists of a series of messages exchanged by client and server in four phases

True

More about SSL handshake (ako treba):

The Handshake Protocol is a process for data transmission in a secure connection, encompassing four phases. In the initial phase, the client initiates the connection and configures security features. Subsequently, the server authenticates itself by sending its certificate, leading to the second phase. The client then verifies the server's certificate and checks parameters in the third phase. Finally, the fourth phase concludes the secure connection setup, with the client transmitting a message to switch to a secure mode.

According to the SSL Architecture (SSL Protocol Stack), the SSL Recodr Protocol provides basic security services to three higher-layer protocols.

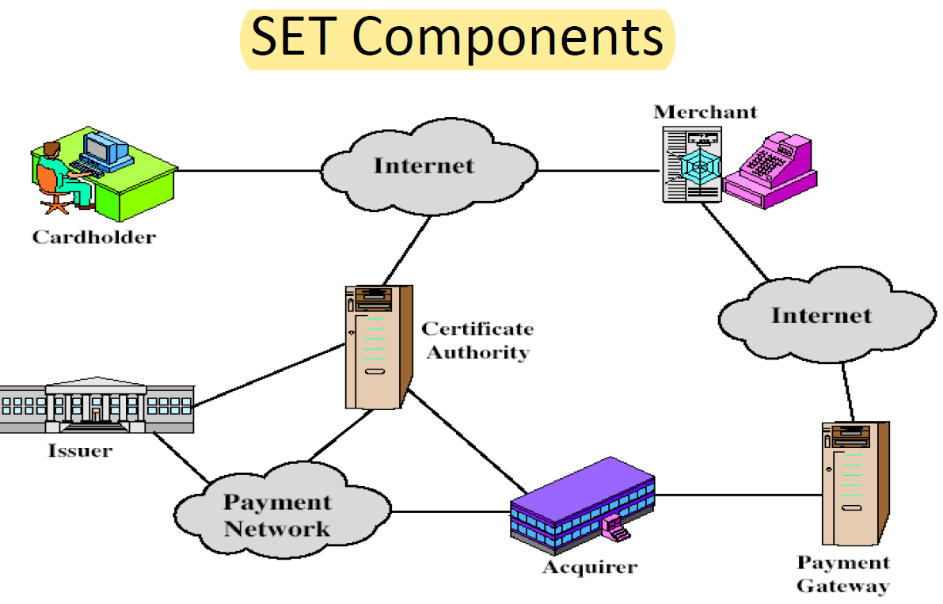
Which are these protocols?

Handshake Protocol is responsible for the initial exchange between the client and server to establish a secure connection, including negotiation of cryptographic algorithms and parameters.

Change Cipher Spec Protocol is a simple protocol that signals a change in the encryption settings for the connection. It indicates that subsequent data will be encrypted using the newly negotiated parameters.

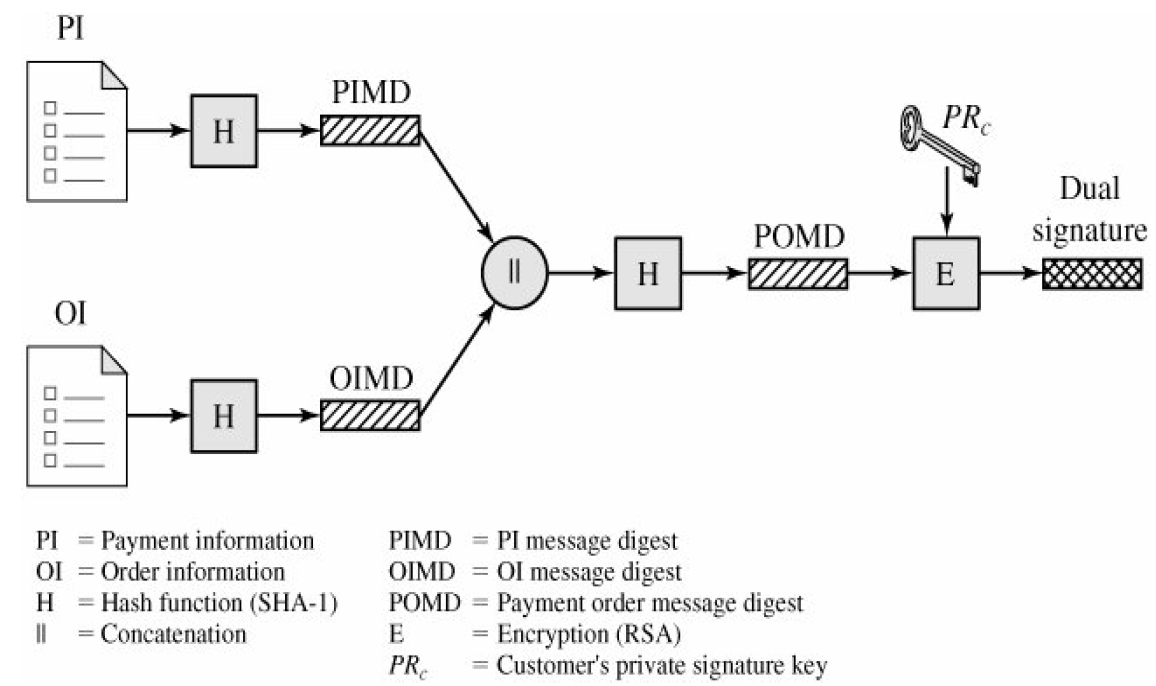
Alert Protocol handles error messages and notifications related to the SSL connection. It can be used to convey information about issues like cryptographic failures or other problems in the connection.

Describe briefly the role of the Acquirer in the Secure Electronic Transactions (SET) Network depicted below



The acquirer provides authorization to the merchant that a given card account is active and that the proposed purchase does not exceed the credit limit. The acquirer also provides electronic transfer of payments to the merchant's account.

Why is the principle of Dual Signature (illustrated below) introduced in Secure electronic Transactions (SET)?



We have two messages Payment information for the band and Order information for the merchant. Neither party needs to know the details of the other but must know that they are linked. The dual signature principle in SET is used to provide a robust mechanism for authenticating both the cardholder and the merchant, ensuring the integrity of the transaction, and enhancing the overall security of electronic payment.