(a)

1. Definition of the certificate of digital signature:

   The certificate is a digital document for offline authentication which verifies the authenticity of the public key of a company, an organization or an individual. CAs(Certificate Authority) are the ones who issue those digital certificate, as everyone trust the Cas whether directly or not. Digital signatures are disapproved if the organization does not have a certificate issued by CA, or the certificate has expired. The certificate contains the identity of the user, such as the name of the organization, the public key of the user, and the time of its validity. The validity is up to three years and more than one year according to the law. There are two types of certificates, signed certificate and self-signed certificate. A signed certificate is created when it's required for being issued to a user by CA, while self-signed certificate is signed by the user itself, which is easy to create and costless. However, websites that use self-signed certificate will not pass the PKI standard, which will warn against https users that the certificate is not verified by the CA. However, it is ok to use self-signed certificate on private web server. Also, the signed certificate issued by CA is verified by the self-signed certificate created by the CA itself.

2. Creation of the certificate of digital signature:

   First, the user or the registration authority will generate keys, the public key will be sent to the registration authority while the private one will be kept by the user, then the registration authority will register the user. Second, the registration authority will verify the user's credential and will also check that whether the public key corresponds to the private

one. Last, the details of verification will be sent to certificate authority by registration authority, who creates the digital certificate and give it back to the user and keeps a copy to itself.

When a web application requires digital certificates, an administrator typically creates digital certificates for each authorized user. The administrator digitally signs each certificate using the system CA certificate.

(b)

X.509 certificate fields:

- version: The version number of the x.509 certificate. (version 1 by default)
- serialNumber: Unique serial number that is created for each certificate that is created by a CA.
- signature: The algorithm used to generate the signature. It must match the signatureAlgorithm.
- issuer: has many subfields such as common_name, country, distinguished_name, locality, organization etc., which describes lists of properties of the issuer.
- validity: Two dates of time—from notBefore (issued date) through notAfter (expiry date).
- subject: has many subfields just as the issuer field, which describes lists of properties of the issuer.
- PublicKey: contains subfields such as algorithm, curve, exponent, size etc., which describes properties of the public key.

(extra) X.509 Version 3 extensions fields:

- extnId: Used to identify this extension.

- critical: A boolean value that is used to inform if the extension is vital or not.
- extnValue: Contains an octet string that could be interpreted freely by a community utilizing an optional extension.

(c)

Virtual private network(VPN), also called secure tunnels, can be set up between firewalls to enable protected connections between secure networks over insecure communication links. All traffic destined to these networks is encrypted between the firewalls. The protocols used in tunneling follow the IP Security (IPsec) standard. For the key exchange between partner firewalls, the Internet key exchange (IKE) standard, previously known as ISAKMP/Oakley, has been defined. The standards also allow for a secure, encrypted connection between a remote client (for example, an employee working from home) and a secure host or network. Authentication is done by the Internet Key Exchange (IKE) server on each end. Instead of using pre-shared key, as it is less secure to packet sniffing, digital certificate is a more secure approach to perform authentication as it doesn’t require pre-shared key being transported in communication. After successful authentication, the IKE servers then negotiate the encryption methodologies and algorithms they will use to secure the VPN connection. Some VPN implementations also require that the certificate contain alternative subject name information, such as a domain name or an e-mail address, in addition to the standard distinguished name information.