(1) At a CA (certificate authority), how a digital certificate is constructed (describe it as a step-by-step procedure to construct one at a CA)?

① This CA includes a merchant’s public key to a text document that describes the profile of the customer.

② This CA calculates the message digest for the text document that contains the public key of the merchant.

③ This CS encrypts the message digest by the secret key of this CA (i.e., this CA digitally signs the message digest).

④ This CA attaches the encrypted message digest to the text document that contains the public key of the merchant.

(2) When a customer downloads a digital certificate of a merchant, how the web browser at the customer uses the digital certificate of the merchant (describe it as a step-by-step procedure at the customer’s web browser)?

① This customer locally calculates the message digest of the text document that contains the public key of the merchant.

② This customer decrypts the encrypted message digest (i.e., the digital signature by the CA) using the CA’s public key.

③ This customer compares the locally calculated message digest and the decrypted message digest.
(3) Which of the following information is (are) not included in a digital certificate (select all that apply)?

(a) The identity of the owner of the certificate in text format
(b) The encrypted algorithm used to encrypt the hash digest of the certificate
(c) The public key of the owner of the certificate
(d) The public key of the CA who issued this certificate
(e) The hash algorithm used to calculate the hash digest for the certificate
(f) None of the above

Only (d).

(4) Regarding the following message:

(a) Why does your browser ask this question to you?

Your web browser couldn’t reach a root CA. Since your browser could not verify the authenticity of this digital certificate, it asks you what you (as the user) would like to do about this digital certificate (you trust it or you throw this digital certificate away).

(b) What is (are) the possible security risk(s) if you accept this digital certificate (i.e., you press “OK” button)? Mention all possible security threat type(s).

This digital certificate can be a bogus digital certificate. If it indeed is a bogus digital certificate, your browser accepts the bogus public key, causing:

- Unauthorized modification (by man-in-middle)
- Release of content messages (by man-in-middle
- Masquerade attack
(5) What are the six security services defined by ITUT-X800 standard?

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation
- Availability of Services.