



“Digital signature scheme”

Self-assessment test

Select the correct answer.

1. Digital signature schemes are based on:
 - Mixed cryptosystems
 - Symmetric key cryptography
 - Hybrid cryptosystems
 - Asymmetric key cryptography**

2. Digital signature provides the following properties:
 - Message integrity, non repudiation and signer confidentiality.
 - Signer authentication and confidentiality, and message integrity.
 - Signer authentication and non repudiation, and message authentication.**
 - Signer authentication, non repudiation, and message confidentiality.

3. In digital signature schemes:
 - The signer uses his public key to sign.
 - The signer uses his private key to sign.**
 - The signer uses the public key of the verifier to sign.
 - The signer uses the private key of the verifier to sign.

4. If a digital signature scheme is deterministic and with appendix:
 - The signatures of two equal messages is the same, and the signatures are attached to the message as a separate part to the message.**
 - The signature of two equal messages is different, and the signatures are attached as a separate part to the message.
 - The signature of two equal messages is the same, and the signatures are embedded in the message.
 - The signature of two equal messages is different, and the signatures are embedded in the message.

-
5. A is signing a message using RSA signing algorithm combined with a hash function. Knowing that the hash value of the message is $H(M)=6$, and that A's public key is $(e,n)=(13,77)$, select the signature value that A computes:
- 12.
 - 74.
 - 41.
 - 37.
6. A receives from B the following message signed with El Gamal signature scheme: $(\{m_i\}; r,s)=(\{9,10,11,12,8,13,1\}; 5,3)$. Select the correct answer considering that B's public parameters are $p=17$, $g=3$, and $Y=14$, and that the hash function is defined as $H(\{m_i\}) = \sum_i m_i \text{ mod. } 13$ (being m_i a set of messages):
- The digital signature is not valid $V_1 \neq V_2=4$.
 - The digital signature is valid $V_1=V_2=4$.**
 - None of the previous answers is correct.
 - All of the above are correct.