

Assignment 5

(Topic 6. Digital Signatures and Identity Based Encryption Topic 7. Security Architecture and Infrastructure)

For the following questions, you may choose three to solve.

1. Suppose that users Alice and Bob carry out the Diffie-Hellman key agreement protocol under an authentic channel with $p = 47$ and $g = 5$. Suppose that Alice chooses her private key $x_A = 3$ and Bob chooses his private key $x_B = 3789$. Determine their public keys respectively. Show the computations performed by both Alice and Bob, and determine the key that they will share.
2. Bob will use RSA signature scheme to sign messages. Let $p = 11$ and $q = 23$. How can Bob generate a digital signature for the message $m = 2$, where the hash function $h(x) = 2x \bmod n$ where $n = pq$? Note. First, Bob should create his public key and private key pair. We omit the certificate step here. Since $n = 11 \times 23 = 253$, $\phi(n) = (p - 1)(q - 1) = 10 \times 22 = 220$. For your convenience, here we list the first ten numbers which are coprime with 220, and their inverses modulo 220.

e	3	7	9	13	17	19	21	23	27	29
$d = e^{-1} \bmod 220$	147	63	49	17	13	139	21	67	163	129

3. For the digital signature standard (DSS) (this type of signatures including ElGamal, ECDSA, GH-DSA or XTR-DSA), the system parameters are $p = 47$, $q = 23$, $g = 2$, the hash function $h(x) = 2x \bmod p$, and PRSG is an LFSR of degree 5.
 - (a) A signer, say Bob, selects his private key and public key pair $(5, 32)$. Suppose that Bob signs the message $m = 101$. Generate a DSS signature of m .
 - (b) What happens if the random number k used in creating the above DSS signature is compromised?
 - (c) DSS specifies that if the signature-generation process results in value of $s = 0$, a new random number k should be generated and the signature should be recomputed? Why?
 - (d) What happens if the hash function is not secure in DSS (this means that for $a = h(m)$, one can easily find another m' such that $a = h(m')$?
4. Continue the above question. Show that the private key x will be compromised if one signs two documents (they may be same) by using the same random number k . Explain it by an example in the ElGamal setting with $p = 107$ and $g = 5$.
5. What is the main difference between public-key cryptography and identity based cryptography?
6. In the public key certificate system, suppose that the certificate authority (CA) employs RSA signature. With the system parameters in question 3 in Part 2, assume that CA's private key and public key pair is given by $(sk_{CA}, pk_{CA}) = (7, 63)$. Bob requests a public-key certificate for his key pair $(sk_B, pk_B) = (19, 139)$ (also RSA key pair).

- (a) How does CA generate the certificate of Bob's public key? (You do not need to actually compute a certificate of Bob's public key, and you only need to specify the format of the certificate.)
- (b) When Alice wishes to send some sensitive information to Bob using Bob's public key, what does she need to do before she performs the encryption using Bob's public key?
- (c) Why a certificate authority is necessary for a public-key system?