

Assignment 5 (Topic 6. Digital Signatures and Identity Based Encryption)

For the following fourth questions, you may choose two to solve.

1. Suppose that users U and V carry out the Diffie-Hellman key agreement protocol with $p = 50147$ and $\alpha = 5$. Suppose that U chooses $x_U = 1367$ and V chooses $x_V = 3789$. Show the computations performed by both U and V, and determine the key that they will share.
2. For RSA signature, let $p = 17$ and $q = 43$. Create a digital signature for the message $m = 161$, where the hashing function is the identity function and the computation at the signer's side is performed by the Chinese Remainder Theory. (You may wish to use Maple or Matlab to do computation.)
3. For the ElGamal type of digital signature (including DSS, EC-DSA, GH-DSA or XTR-DSA),
 - (a) What happens if a random number k used in creating a ElGamal (or DSS) signature is compromised? Explain this by an example in the DSS setting with $p = 47$, $q = 23$ and $\alpha = 7$.
 - (b) 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?
4. 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 $\alpha = 5$.
5. What is the main difference between public-key cryptography and identity based cryptography?