06-88-447: Computer Networks and Security, Summer 2017

Assignment four (Due: Sunday July 30, 2017)

Programming is recommended for solving Problem 1(b).

1. Bob sets up an RSA system by choosing $p = 17$ and $q = 19$. Bob selects the public key as $e = 11$.
   - (a). Solve Bobs private key d.
   - (b). Bob wants to put digital signature on the document $m = 101$ with message digest $h(m) = 3$. Give the steps for signing phase and solve y.
   - (c). Assume Alice wishes to verify whether or not the document $m = 101$ is signed by Bob. Give the steps for verification phase with necessary calculated results.
2. Bob has an RSA system with public key $(n, e) = (133, 11)$. Alice wish to share a secret session key $k = 2$ with Bob by using key distribution scheme with RSA encryption. Elaborate the steps performed by Alice and Bob with the calculated results.
3. Alice and Bob wish to use Diffie-Hellman key exchange scheme to share a secret session key between them. They both agree upon choosing the public information GF(19) with primitive element $\alpha = 2$. If Alice chooses random number $a = 7$ and Bob selects $b = 4$, decide their shared session key.
4. Alice and Bob would like to set up a secret session key between them before they can transmit confidential data to each other. Both Alice and Bob agree to use Diffie-Hellman key exchange scheme with GF(2^5), $f(x) = x^5 + x^2 + 1$, and $\alpha = x$. Show the detailed steps Alice and Bob perform to obtain the session key. (Assume that Alice chooses $a = 5$ and Bob chooses $b = 7$)