MAS433 Cryptography: Tutorial 7
Digital Signature
11.11.2011

Instructions.

1. Submission of tutorial solution is compulsory.
2. Submission deadline: 10 November 2011, 6PM
3. Please submit your solution by sending email to wuhj@ntu.edu.sg (If your solution is handwritten, you can scan and convert it into digital format, such as .pdf document.)
4. Tutorial solution will not be provided after the tutorial class.

Question 1. RSA Signature Scheme
Suppose that hash function is not used in RSA digital signature scheme. The signature is generated as $s = m^d \mod n$. Given a message m and its signature s, how to modify m without being detected?

Question 2. ElGamal Signature Scheme

2.1 In the Elgamal signature scheme, why should the signature with $s = 0$ be deleted? Is this requirement useful in practice?

2.2 In the Elgamal signature scheme, each per-message secret integer k should be used only once. If the per-message secret integer k is reused, how to attack this digital signature algorithm?

2.3 In the Elgamal signature scheme, each per-message secret integer k should be randomly generated. If the per-message secret integer k is generated as follows: k_0 is randomly generated, $k_{i+1} = k_i + a$, where a is a known constant. Develop an attack to recover the private key.

2.4 In the ElGamal signature scheme, each per-message secret integer k should be randomly generated. If the per-message secret integer k is generated as follows: k_0 is randomly generated, $k_{i+1} = k_i + a$, where a is a large unknown constant. Develop an attack to recover the private key .

Question 3. Digital Signature Algorithm (DSA)

3.1 In the Digital Signature Algorithm, if the per-message secret integer k is reused, how to attack this digital signature algorithm?

3.2 In a modified DSA, s is generated as $s = k^{-1}(H(m) - xr) \mod q$. What is the signature verification algorithm for this modified DSA?

3.3 Let p and q be prime numbers and q is a divisor of $p - 1$. Show that for any integer t, if $g = h^{(p-1)/q} \mod p$, then $g^t \mod p = g^{t \mod q} \mod p$.

3.4 (Bonus Question) Explain why the size of q is at least 160 bits, and why the size of p is at least 1024 bits in DSA.

Question 4. Public key certificate.

4.1 In secure shell (SSH), the public key certificate is not used. What is the risk?

4.2 When you connect to a website secured by TLS/SSL, if you notice that the public key certificate of that website is invalid (a warning window would appear if the certificate is invalid), and you continue to access that website, what is the risk?

Question 5. Unconditionally secure and computationally secure
Is there unconditionally secure public key cryptosystem? Briefly explain why.