MAS433 Cryptography: Tutorial 5
Key Establishment and Management
03.12.2010

Problem 1. Randomness in key generation.
Suppose that the key generation process is biased. Each key bit is independently generated, but the value of each key bit is '1' with probability 0.95. Suppose that the key size is 64 bits.

1.1 What is the entropy of each key bit?

1.2 What is the entropy of the key?

1.3 What is the probability that 64 bits in a key with values '1'?

1.4 What is the probability that at least 63 bits in a key with values '1'?

1.5 What is the probability that at least 62 bits in a key with values '1'?

1.6 What is the probability that at least 61 bits in a key with values '1'?

1.7 In Problem 1.6, how many keys have at least 61 bits with values '1'? Write your result in the form of $2^{x.x}$.

1.8 Compare the results of Problem 1.2 and 1.7 . Explain how the entropy of a key is related to the strength of the key.

Problem 2. Public key certificate.

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

2.2 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?

Problem 3. Secret Sharing.
Alice is using the RSA digital signature scheme. Her public key is (n, e), and her private key is d. Alice uses the following scheme to protect her private key: generate three integers d_1, d_2, d_3 in $[0, n-1]$ so that $d_1 + d_2 + d_3 \equiv d$. After storing each d_i on a trusted server S_i $(1 \leq i \leq 3)$, Alice deletes her private key x.

3.1 To sign a message m, Alice sends $H(m)$ (the message digest of m) to each server S_i $(1 \leq i \leq 3)$, and each server S_i performs a local computation and sends T_i to Alice. Given T_1, T_2, T_3, Alice generates the signature without reconstructing her private key. Explain how server S_i computes T_i and how Alice generates the signature.

3.2 To provide fault tolerance, Alice shares her private key d among the three servers so that any two of the three servers can be used to sign messages without reconstructing her private key d, but the signature cannot be generated with only one server. Explain how to share the private key d, and how to sign a message.