Information Theoretic Security

Fall semester, 2013

Assignment 2

Assigned: Thursday, September 26, 2013

Due: Wednesday, October 9, 2013

Somayeh Salimi

Problems

Problem 1.1:

Suppose that in a public key framework, Alice and Bob have key pairs (K_{pu}^A, K_{pr}^A) and (K_{pu}^B, K_{pr}^B), respectively (subscript pu is referred to public key and the subscript pr is referred to private key). Alice intends to send message m to Bob. Give a scheme to sign the message and simultaneously securing that (providing confidentiality of the message).

Problem 1.2:

One approach to share a secret key between two entities is DiffieHellman key exchange protocol instead of establishing a secure channel between them. Describe this protocol. How is "the Man in the Middle Attack"resolved in this protocol?

Problem 1.3:

Each of AH and ESP protocols of IPsec can work in two modes; TRANSPORT and TUNNEL. Describe these two modes of IPsec and their differences.

Problem 1.4:

Show that the perfect security is compromised if two different messages are encrypted with a same key in One-Time Pad algorithm (which is described in slide #7 of the second lecture).

Problem 1.5:

Show that to provide perfect secrecy in One-Time Pad algorithm, the redundancy should be completely removed from the keystream (suppose that in key stream $K = (k_1, k_2, ..., k_n)$ there is correlation between i-th and j-th bits as $k_i = k_j \oplus e$ where e is a binary random variable such that $\Pr\{e = 1\} = p$ where $0 \leq p < \frac{1}{2}$) and show that the perfect security is compromised, i.e., $I(M; C) \neq 0$).

Problem 1.6:

Describe the relation between the three properties of the hash functions (pre-image resistance,

weak collision resistance and strong collision resistance), which implies the other one?