Data Security 23.3.2009

1. For $P = (0,1) \in EC_5(2,1)$, $2P = (1,3)$, $3P = (3,3)$, $4P = (3,2)$, $5P = (1,2)$, $6P = (0,4)$, $7P = O$. A uses 3 as secret key and B uses 5 as secret key. What are their public keys in El Gamal encryption. A sends message (1,2) to B encrypted. What is the encrypted message. (4p)

2. Sign message "YES". Hash the message by splitting it to 4-bit blocks and bitwise XORing the blocks. In signing use RSA constructed of the primes $p = 3$ and $q = 11$, and the public encryption key $e = 3$. The ASCII codes of Y, E, and S in hexadecimal are 59, 45 and 53. (4p)

3. The following authentication protocol uses authentication center X, public key encryption, and random numbers R for secret key distribution. Explain the meaning and the purpose of the phases and the sent data. Is the protocol secure against replay attack? (4p)

   (a) $A \rightarrow X: \; A \circ B \circ R_A$

   (b) $X \rightarrow A: \; E_{J_A}(B \circ R_A \circ K_S \circ E_{J_B}(A \circ K_S))$

   (c) $A \rightarrow B: \; E_{J_B}(A \circ K_S) \circ E_{K_S}(R'_A)$

   (d) $B \rightarrow A: \; E_{K_S}(R'_A + 1) \circ E_{K_S}(R_B)$

   (e) $A \rightarrow B: \; E_{K_S}(R_B + 1)$

4. Answer briefly (1p each):

   (a) What is GnuPG program used for?

   (b) What does double signature of SET paying mean and why is it used?

   (c) On what TCP/IP layer does IPsec work and what does it imply?

   (d) What does zero information proof mean and for what can it be used?