Quiz 4, IS2935, October 10, 2003

1. Alice wants to communicate with Bob. Let (E_A, D_A) and (E_B, D_B) be public-private key pairs of Alice and Bob. Alice wants to send a message to Bob. In the table, indicate the encryption expression that Alice and Bob would use when Alice sends message M to Bob for each requirement.

   Use ($E(M)$ and $D(M)$ to represent encryption using public and private keys of a message M. Let c be the cipher-text that Bob receives. **[3]**

[a]	To ensure confidentiality	Alice does: $c = E_B(M)$ Bob does: $D_B(c)$
[b]	To ensure integrity/authentication	Alice does: $c = D_A(M)$ Bob does: $E_A(c)$
[c]	To ensure both authentication and confidentiality	Alice does: $c = E_B(D_A(M))$ Bob does: $E_A(D_B(c))$

2. Consider the message blocks m_1, m_2, m_3. If the Cipher Block Chaining mode DES encryption can be expressed as follows:

$$c_1 = \text{DES}(m_1 \oplus ivector),\ c_2 = \text{DES}(m_2 \oplus c),\ c_3 = \text{DES}(m_3 \oplus c_2)$$

   where *ivector* is the initial vector and $\oplus$ is the XOR operation

   write the expressions for the DES decryption to extract each of the message blocks m_1, m_2, and m_3. **[3]**

Answer:

$$m_1 = \text{DES}(c_1) \oplus ivector,$$
$$m_2 = c_1 \oplus \text{DES}(c_2),$$
$$m_3 = c_2 \oplus \text{DES}(c_3),$$

(Note: Previous version was slightly different and contained less information. So 1.5 points have been awarded to all for this question – remaining 1.5 points have been awarded based on your response)

3. What do you understand by a cryptosystem being "computationally secure"? **[1]**

Answer:

- Cost of breaking a ciphertext exceeds the value of the hidden information
- The time taken to break the ciphertext exceeds the useful lifetime of the information

4. Write the simple key exchange protocol involving Alice, Bob and the trusted party Cathy, where Bob initiates the communication (with Cathy to get the session key). **[3]**

(**Answer**: see lecture 6 slides)