# Final Exam

December 11, 1995

Name: _____

1. (a) Draw a diagram for a communication between Alice and Bob using DES in electronic codebook (ECB) mode. Use the labels $x_i$, $y_i$ for the plaintext and ciphertext respectively.

   (b) Assume one pair of plaintext/ciphertext $(x_i, y_i)$ is known. How many steps are required for a brute force attack in a worst case scenario?

   (c) Draw a diagram for a communication using the cipher block chaining (CBC) mode.

   (d) What is the minimum number of pieces of (i) plaintext and (ii) ciphertext that are needed for a brute force attack in CBC mode?

   (e) How many steps are required for a brute force attack in a worst case scenario?

   (f) Why is the CBC mode more secure than the ECB mode in many applications? (If you wish, you can demonstrate your answer with an example.)

2. You are asked to set up an RSA cryptosystem. The parameters $p = 17$ and $q = 19$ are given.

   (a) Which of the two values $b_1 = 33$ and $b_2 = 35$ can be used as the parameter "$b$" in the RSA scheme?

   (b) Use the valid $b$ from above and provide the public key $K_{pub} = (n, b)$ and the private key $K_{pr} = (p, q, a)$. If you weren't able to do part (2a), use $b = 49$.

3. Bob sends a message to his friend Alice, encrypted with the ElGamal encryption scheme. Foolishly, he keeps the parameter $k$ the same for all encryption processes. Our favorite bad guy, Oscar, knows that Bob's first message is always his terminal number, so that $x_1 = 22$. Oscar observes the following two ciphertext messages:

$$(y_{11} = 6, y_{12} = 17)$$
$$(y_{21} = 6, y_{22} = 25)$$

   The system parameters are $p = 31$, $\alpha = 3$, $\beta = 18$.

   Oscar can now determine $x_2$. What is the second piece of cleartext $x_2$ that Bob has sent?

4. We consider a cryptosystem based on the elliptic curve:

$$y^2 \equiv x^3 + x + 6 \bmod 11 \tag{1}$$

The public key $K_{pub} = (\alpha, \beta)$ has the values $\alpha = (8, 3)$ and $\beta = (2, 4)$. The private key is $K_{pr} = a = 4$.

   (a) What are the coefficients $a$ and $b$ *of the curve equation* (1)?

   (b) You receive the ciphertext $(y_0, y_1, y_2) = ((3, 5), 2, 10)$. Decrypt the ciphertext and determine the plaintext values $(x_1, x_2)$. Use the addition formulas for decryption. (Hint: Observe that the parameter "a" in the formula for point doubling is the coefficient from the curve equation and *not* the private key $K_{pr}$.)

5. In this problem the complexity of the encryption process for elliptic curve cryptosystem is investigated.

   (a) Describe an adaption of the square-and-multiply algorithm to the operation

$$y = k \cdot \alpha \tag{2}$$

   where $k$ is an integer and $\alpha$ and $y$ are points on the curve. Provide a pseudo-code description. Assume there is a function `ellc_add(a, b)` which performs addition on elliptic curves and returns the sum `a + b`.

   (b) How many (i) point additions and (ii) how many point doubling are required on average for the operation (2), assuming that $k$ has $\log_2 p$ bits?

   (c) How many group operations are required for encrypting the message pair $(x_1, x_2)$ on average? Addition and doubling count each as one group operation. Take only the operations for computing $c_1$ and $c_2$ and for $y_0$ into account (the complexities for computing $y_1, y_2$ are negligible.)

   (d) Assume that $k$, $p$, $x_1$, and $x_2$ each have $\log_2 p = 160$ bits and that each group operation (addition or doubling) requires 20 $\mu$sec. What is the data throughput of the encryption unit in bits/sec? (Or, formulated differently: How many bits of cleartext can be encrypted per second?)

6. (a) Briefly describe the meaning of the terms C(U), ID(U), $a_U$, $b_U$ $K_{UV}$, $sig_{TA}$, $ver_{TA}$ in the Diffie-Hellman key predistribution scheme. It is not necessary to provide a functional description of every term — do not write more than one sentence per term. (For instance, something like "$x_y$ is the private key of user $y$" is sufficient.)

   (b) Provide the basic protocol which is executed in oder to establish a common secret key between Alice and Bob using the Diffie-Hellman key predistribution scheme. Use the variables C(A), ID(A), $a_A$, $K_{AB}$, $sig_{TA}$, $ver_{TA}$, and their B counterparts in the protocol.

   (c) The system parameters are $p = 61$ and $\alpha = 18$. Alice's private key is $a_A = 8$ and Bob's is $a_B = 4$. What is the common key $K_{AB}$ which Alice and Bob establish?

   (d) We consider now an attack on the scheme where Oscar is an active opponent. In the first stage of the protocol Alice obtains Bob's certificate. Assume that Oscar replaces Bob's public key $b_B$ in the certificate with his own key $b_O$. Will this manipulation be detected? If so, where in the protocol?

7. We consider now a successful "man in the middle attack" against the Diffie-Hellman key predistribution scheme. Assume that Oscar gets access to the secret signature algorithm $sig_{TA}$ of the TA. Also assume that he has unlimited read and write access to the central data base. Furthermore assume that Oscar can manipulate the channel (active attack.)

   Oscar is now capable of performing manipulations such that instead of establishing a session key $K_{AB}$ between Alice and Bob, there are two session keys $K_{AO}$ (between Alice and Oscar) and $K_{BO}$ (between Bob and Oscar). Alice and Bob, however, are not aware of the manipulation and still think that they share a secret session key.

   Describe in detail what Oscar has to do in order to run the attack successfully. Show how Oscar can then read and alter a message sent from Alice to Bob.