Final Exam

December 13, 1999

Name: _____

1. Lenstra/Verheul assumed for their key size comparison that DES was considered adequately secure in 1982. If we agree with this assumption, what is the recommended key bit length for a symmetric cipher in the year 2000?

2. On the first glance it seems as though a brute force attack against a short message encrypted with a one-time pad is feasible. This is a paradox since we know that the OTP is unconditionally secure. Describe why a brute force attack, e.g., against a 40 bit long ciphertext, does not work. Remark: You have to resolve the paradox! That means answers such as "The OTP is unconditionally secure and therefore a brute force attack does not work" is not a valid one and will get no points.

3. Given is a Diffie-Hellman key exchange protocol with the modulus $p = 107$ and the element $\alpha = 4$.

   (a) What is the order of α in $Z^{\star}_{107}$? (Hint: Consider which orders are possible in the group.)

   (b) Your private key is 167. Compute the public key. Note that you can compute this one much faster than evaluating α^{167} directly.

4. Given is a Menezes-Vanstone elliptic curve encryption scheme with the parameters:

$$\begin{aligned} y^2 &= x^3 + x + 13 \bmod 31 \\ \alpha &= (9, 10) \\ \beta &= (18, 29) \end{aligned}$$

   Your private key is $a = 2$. You receive the message $((23, 19), 1, 24)$. What are the two pieces (x_a, x_b) of cleartext?

5. At the end of an elliptic curve Diffie-Hellman key exchange protocol Alice and Bob share a secret point $R = (x, y)$. The modulus of the elliptic curve is a 160 bit prime.

   (a) Why should only the x coordinate of R be used as session key for a symmetric cipher?

   (b) We now want to provide a session key for a block cipher with 320 key bits. We apply a hash function H with 320 bits of output. We compute the session key as

   $$K_{AB} = H(x \parallel y)$$

   (i) Describe in general terms how an exhaustive key search against the symmetric cipher would be performed *most efficiently*. You do not have to get into mathematical details, but rather provide a step-by-step description of what has to be done. (ii) How many key tests are required for the attack in the worst case? (iii) Comment on the cryptographic strength of the block cipher with this key establishment method.

6. Why does sender (or message) authentication imply data integrity? Is the opposite true too, i.e., does data integrity imply sender authentication? Justify both answers.

7. In an RSA digital signature scheme Alice signs messages x and sends them together with the signature y to Bob. Alice's public key is the pair (n, b), and her private key is a.

   Oscar can perform man-in-the-middle attacks. His goal is to alter messages and provide them with a digital signature which will check out correctly on Bob's side. Show everything that Oscar has to do in a successful attack.

8. Given is a user domain in which users share the Diffie-Hellman parameters α and p. Each user's public Diffie-Hellman key is certified by a CA. Users communicate securely by performing a Diffie-Hellman key exchange and then encrypting/decrypting messages with a symmetric algorithm such as 3DES.

   Assume Oscar gets hold of the CA's signature algorithm, which was used for generating certificates. Can he now decrypt old ciphertexts which were exchanged between two users before the CA signature algorithm was compromised, and which Oscar had stored? Explain your answer.