# Final Exam

December 9, 1997

Name: _____

1. One popular approach for providing security on the Internet are firewalls. Firewalls are put between a local area network and the Internet connection. Although in widespread use in practice, there are general drawbacks/limits associated with firewalls. Briefly discuss some of them.

2. Given is the following string of ciphertext which was encrypted with an affine cipher

   `JNNDLBVNEXGBO`

   You know that the first plaintext letter is a `C` and that the last one is an `R`.

   Find the coefficients $c$ and $d$ such that

   $$x = c\,y + d \bmod 26$$

   and decrypt the message.

3. The main operation in elliptic curve cryptosystems is the multiplication of a point $P$ on the curve by an integer. Show the steps that are being performed for calculating

   $$136\,P$$

   through an adaption of the square and multiply algorithm.

4. Given is an elliptic curve cryptosystem with a prime modulus $p \approx 2^{200}$. The system is used for a Diffie-Hellman key exchange. Assume that the public keys have already been computed.

   The time for point addition or point doubling is 250 $\mu$s. How long does it take to compute the session key in the Diffie-Hellman key exchange protocol for one party on average?

5. Given is an ElGamal signature scheme with $p = 31$, $\alpha = 3$ and $\beta = 6$. You receive the message $x = 10$ twice with the signatures $(\gamma, \delta)$:

$$\begin{array}{ll} (i) & (17, 5) \\ (ii) & (13, 15) \end{array}$$

   (a) Are both signatures valid?

   (b) How many valid signatures are there for each message $x$ and the specific parameters chosen above?

6. Describe in general terms:

   (a) What are certificates (structure, functionality)?

   (b) Why are certificates frequently being used in public-key schemes?

7. We consider a protocol in which messages are not encrypted but sent in cleartext. Each message, however, is hashed and then digitally signed. The signature $y$ is sent together with each message $x$.

   Assume now that Oscar is able to find a collision in the hash functions, i.e., he can find $x'$ such that

$$h(x) = h(x')$$

   He can also (within limits) control the contents of $x'$.

   Describe how Oscar can now alter Bob's messages such that Alice will still consider them valid messages from Bob.

8. Given is an RSA encryption scheme in which Alice has a public and private key pair. Show how Oscar can run a man-in-the-middle attack which allows him to read an alter encrypted messages that are sent from Bob to Alice without detection by Alice.