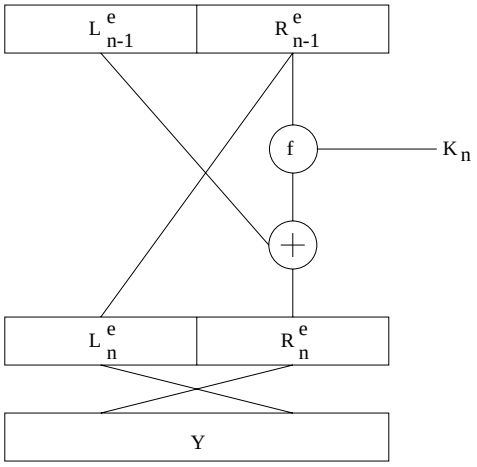
Final Exam

December 9, 1996

Name: _____

1. Many block ciphers such as DES are based on Feistel networks. One central reason for building ciphers from Feistel networks is that encryption and decryption are almost identical operations. We will study this characteristic in the following problem.



   (a) Given is the last round of an n-round Feistel network. Draw the first round of the corresponding decryption network. Use superscripts "d" to denote the variables.

   (b) Show that $L_1^d = R_{n-1}^e$ and that $R_1^d = L_{n-1}^e$.

   (c) Express L_n^d and R_n^d through values from the encryption operation.

2. What is the discrete logarithm problem in $Z_p^\star$? What is the Diffie-Hellman problem in $Z_p^\star$? How are the two problems related?

3. Your task is to compute a session key in a Diffie-Hellman key exchange protocol based on elliptic curves. Your private key is $a_A = 6$. You receive Bob's public key $b_B = (5, 9)$. The elliptic curve being used is

$$y^2 \equiv x^3 + x + 6 \bmod 11.$$

4. We consider the performance of an ElGamal digital signature scheme with $\lceil \log_2 p \rceil = 768$. Our timing model assumes that multiplication or squaring modulo p of an n-bit number takes $(\lceil n/32 \rceil)^2$ clock cycles. What is the required clock rate if we want to perform one signature verification in not more than 100 msec on average?

5. We consider an attack against the RSA signature schemes. Given are the parameters of Alice's signature, $n = 10403$, and the verification key $k_{\text{pub}} = 129$.

   (a) You are Oscar. Construct a message/signature pair which can be verified as "correct". Any signature y except $y = 1$ is allowed.

   (b) Why is this attack of limited importance in practice?

6. Describe in general terms:

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

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

7. Oscar manages to bribe the trusted authority in the Diffie-Hellman key predistribution scheme. The TA replaces Bob's public key b_B in Bob's certificate by b_o, which is known by Oscar, and signs it correctly.

   (a) Is Oscar now able to perform a general (i.e., reading and altering of encrypted messages from Alice *and* Bob) man-in-the-middle attack which goes undetected by Alice and Bob?

   (b) What kind of undetected attack can Oscar perform? Exactly describe the limitations of this attack.

8. (a) Describe an attack against which time stamps protect.

   (b) Draw a simple protocol for a time stamp service involving Alice and a trusted authority. Assume a message x (to be time-stamped), a public hash function h, the signature algorithm sig_{TA} of the TA, and a time stamp TS.