Final Exam

December 16, 1998

Name: ____________________

1. The proposed IPsec security protocol has two main parts, the Authentication Header Protocol and the Payload Encapsulation Protocol. Briefly describe what these protocols do.

2. A linear shift feedback register (LFSR) of degree m is described by:

$$z_{i+m} = \sum_{j=0}^{m-1} c_j \, z_{i+j} \bmod 2 \quad , \quad 0 \leq i$$

   where z_k are the outputs and the c_j are the m binary feedback coefficients.

   Breaking and LFSR means to determine the m unknown coefficients c_j, $0 \leq j \leq m-1$, by observing the output bits z_k. We assume we know m. **Derive** the matrix equation for breaking the LFSR of degree m with $2m$ known outputs z_k.

3. Given is a Diffie-Hellman key exchange algorithm. The modulus p has 1024 bits and α is generator of a subgroup, where $\text{ord}(\alpha) = o \approx 2^{160}$.

   (a) What is the maximum value that the private keys should have?

   (b) How long does the computation of the session key take on average if one modular multiplication takes 700 μsec, and one modular squaring 400 μsec? Assume that the public keys had already been computed.

   (c) One well known acceleration technique for discrete logarithm systems uses short primitive elements. We assume now that α is such a short element (e.g., a 16 bit integer). Assume that modular multiplication with α takes now only 30 μsec. How long does the computation of the public key take now? Why is the time for one modular squaring still the same as above if we apply the square and multiply algorithm?

4. Given is an ElGamal crypto system. Bob tries to be especially smart and chooses the following pseudo random generator to compute new k values:

$$k_i = k_{i-1} + f(i) \quad , \quad 1 \leq i \tag{1}$$

where $f(i)$ is a "complicated" but known pseudo random function. (For instance, $f(i)$ could be a strong hash function such as SHA or RIPE-MD160.) k_0 is a true random number that is not known to Oscar.

Bob encrypts n messages x_i as follows

$$\begin{aligned} y_{1,i} &= \alpha^{k_i} \bmod p, \\ y_{2,i} &= x_i\, \beta^{k_i} \bmod p, \end{aligned}$$

where $1 \leq i \leq n$. Assume that the last cleartext x_n is known to Oscar and all ciphertext.

Provide a formula with which Oscar can compute any of the messages x_i, $1 \leq i \leq n-1$. Of course, following Kerckhoff's principle, Oscar knows the construction method shown in (1), including the function $f()$.

5. There is an attack against the ElGamal digital signature scheme in which Oscar can construct a valid signature for a random message. Your task is to finish the attack described in the following.

Given are Alice's set-up parameters p, α, β. Oscar chooses integers i and j, where $0 \leq i, j \leq p-2$, and $\gcd(j, p-1) = 1$. He then computes

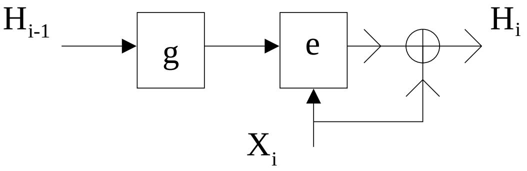
$$\begin{aligned} \gamma &= \alpha^i \beta^j \bmod p \\ \delta &= -\gamma\, j^{-1} \bmod (p-1) \end{aligned}$$

   (a) How must x be constructed so that Bob verifies the signature correctly (general expression)?

   (b) Why is this attack of limited use?

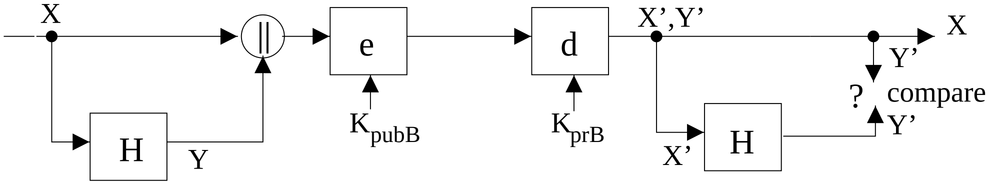
   (c) Using the values $p = 467$, $\alpha = 2$, $\beta = 132$, $i = 10$, and $j = 7$, compute x and the signature (γ, δ) that would be verified correctly. Note that you do *not* have to do the actual verification.

6. Consider the following hash function



Why is the use of DES for the encryption function e a bad idea?

7. Given is the system shown below which uses a (publicly known) hash function H and public-key encryption/decryption.



Which of the following security services are provided: privacy, sender authentication, integrity, non-repudiation? For each security service, explain (briefly) **why** it is provided.

8. In this problem we study the consequences if faked public CA keys have been issued. As an example we consider an authenticated RSA encryption system.

   (a) First, show how an authenticated RSA encryption system works if Alice has the *correct* verification key ver_{CA}. Assume Alice sends an encrypted message to Bob. Do not assume any Oscars for this part of the problem. Furthermore, assume that Bob's public and private key have already been computed, and the public key has been certified correctly by the CA.Use the variables (b_B, n_B) for Bob's public key and a_B for Bob's private key.

   (b) Assume now Oscar was in the set-up phase of the system capable of giving Alice his public verification key ver_O rather than the one of the CA, without Alice noticing it.

   Alice wants again to encrypt a message and send it to Bob as above. Show all steps of a protocol in which Oscar runs a man-in-the-middle attack such that he can read (and alter) encrypted messages from Alice to Bob, without Alice or Bob noticing it. Start with Alice's attempt to get Bob's public key.