Fall 2000 EE578/CS578 Prof. Christof Paar

Final Exam

December 13, 2000

Name: ________________________________

Problem	1	2	3	4	5	6	7
Points							

1. Briefly explain the meaning of the following two mechanisms of IPSec: (i) Authentication Header (AH) and (ii) Encapsulating Security Payload (ESP).

2. We use the affine cipher for encryption and decryption. We base our cipher on an ancient alphabet which consists of 273 symbols. What is the key space of the cipher? Note that 7 divides 273.

3. We consider Rijndael with 128 bit block length and 128 bit key length. What is the output of the first round of Rijndael if the cleartext consists of 128 ones, and the first round key (i.e., the first sub-key) also consists of 128 ones? You can write your final results in a rectangular array format if you wish.

4. Given are the following parameters of the RSA cryptosystem: the primes are $p = 101, q = 107$, and the public key is $b = 4497$. You receive the ciphertext $y = 7411$. Compute the cleartext.

5. Given is a Diffie-Hellman key exchange protocol with the modulus $p = 131$ and the element $\alpha = 70$.

   (a) What is the order of α in $Z^{\star}_{131}$?

   (b) Your private key is 774. Compute the public key as efficiently as possible.

6. Given are two protocols in which the sender's party performs the following operation:

   (a) Protocol A:
   $$y = e_{k_1}[x||H(k_2||x)]$$
   where x is the message, H is a hash function such as SHA-1, e is a private-key encryption algorithm, "||" denotes simple concatenation, and k_1, k_2 are secret keys which are only known to the sender and the receiver.

   (b) Protocol B:
   $$y = e_k[x||sig_{k_{pr}}(H(x))]$$

   Provide a step-by-step description (e.g., with an itemized list) of what the receiver does upon reception of y. You may want to draw a block diagram for the process on the receiver's side, but that's optional.

7. State whether the following security services:

   - confidentiality
   - integrity
   - non-repudiation

   is given for each of the two protocols given in the previous problem. You have to justify your answer in every case (1-2 sentences every time can be sufficient).