Problem Set #7

CMSC/Math 456
Instructor: Daniel Gottesman

Due on Gradscope, Thursday, Nov. 9, noon (before start of class)

General instructions: If you collaborate or use any outside resources, remember to cite them in your solutions.

Problem #1. Three-Party Key Agreement (60 points)

In this problem, three people (Alice, Bob, and Charlie) want to agree on a single secret key k that will be known to all three of them but unknown to Eve. When one person "announces" something, it is heard by the other two people and also by Eve. Thus, if Alice announces something, Bob and Charlie hear it, as well as Eve. You do not need to analyze security in these protocols beyond a superficial level (i.e., do not do something obviously insecure like send the key as plaintext).

a) (20 points) Alice, Bob, and Charlie use Diffie-Hellman to agree on the key: The protocol has a pre-arranged g and p, as usual for Diffie-Hellman. Alice chooses a random secret value a (known only to her) and announces $A = g^a \bmod p$. Bob chooses a random secret value b (known only to him) and announces $B = g^b \bmod p$. Charlie chooses a random secret value c (known only to them) and announces $C = g^c \bmod p$. Then, Alice computes and announces $A' = C^a \bmod p$, Bob computes and announces $B' = A^b \bmod p$, and Charlie computes and announces $C' = B^c \bmod p$. What should Alice, Bob, and Charlie do to discover a shared secret key k without any further communication (either announcements or private communications).

b) (20 points) In this variation, Alice already has Bob and Charlie's public keys for Diffie-Hellman/El-Gamal-based KEM. Is there a way for the three of them to agree on a single key using only an announcement (of any polynomial length) by Alice? How or why not?

c) (20 points) Alice, Bob, and Charlie wish to reduce the amount of communication they need. Alice already has Bob and Charlie's public keys for RSA-based KEM. Is there a way for the three of them to agree on a single key using only an announcement (of any polynomial length) by Alice? How or why not?

Problem #2. Alternative Padding Methods for RSA (60 points)

In this problem, we will investigate the security of some alternative methods of padding messages for RSA. In all cases, assume the public key is $(N, e = 3)$, and let $n = \lfloor \log N \rfloor$. All padding methods are described by taking the message m to be written in binary and using $||$ to represent concatenation of bit strings.

a) (15 points) Pad by adding $\lceil \log n \rceil$ random bits to the beginning of the message. I.e., if the random bits are r, then $\tilde{m} = r||m$, and the message is $n - \lceil \log n \rceil$ bits long. Find an attack to show that this encryption method is insecure.

b) (15 points) Pad by adding $\lfloor n/4 \rfloor$ random bits to the end of the message. I.e., if the random bits are r, then $\tilde{m} = m||r$, and the message is $\lceil 3n/4 \rceil$ bits long. Find an attack to show that this encryption method is insecure. **Hint:** Try a low-m attack.

c) (15 points) Let padding method A be to add $\lfloor n/4 \rfloor$ random bits to the beginning of the message. I.e., if the random bits are r, then $\tilde{m} = r || m$ and the message is $\lceil 3n/4 \rceil$ bits long. Let padding method B be to add $\lfloor n/4 \rfloor$ random bits to the beginning of the message and another $\lfloor n/4 \rfloor$ random bits to the end of the message. I.e., if the first set of random bits is r and the second set is r', then $\tilde{m} = r || m || r'$ and the message is $\lceil n/2 \rceil$ bits long. Show that if method A is secure, then method B is secure.

d) (15 points) In this padding method, the message has a variable length ℓ, with $n/4 \leq \ell \leq 3n/4$. Pad by adding $n - \ell$ random bits to the beginning of the message. I.e., if the random bits are r, then $\tilde{m} = r || m$. There is a problem with this padding method. What is wrong with it?