UConn, School of Computing
Fall 2024
CSE 3400/CSE 5850: Introduction to Computer and Network Security / Introduction to Cybersecurity

Assignment 5

Instructor: Prof. Ghada Almashaqbeh
Posted: 11/8/2024
Submission deadline: 11/17/2024, 11:59 pm

Notes:

- Solutions **must be typed** (using latex or any other text editor) and must be submitted as a pdf (not word or source latex files).

Problem 1 [30 points]
This problem is about shared key protocols:

1. For the 2PP protocol in slide 16, lecture 8, we modify the protocol as follows: the nonce sent by Bob is computed as $N_B = 3 \cdot N_A$. Eve, is a MitM attacker who is trying to impersonate Alice, i.e., claim to be Alice and complete a successful handshake with Bob. How can Eve do that under this modified protocol? Justify you answer.

2. For the 2PP protocol in slide 16, lecture 8, Eve is a MitM who has planned the following attack. Every time Alice sends a nonce N_A (i.e., the first message), Eve modifies that nonce to another value she chooses and then send the modified value to Bob. Why is Eve able to do that? what is the impact of this attack on Alice and Bob? Justify you answer.

3. For the 2RT-2PP protocol in slide 7, lecture 9, Charlie wants to modify the protocol by replacing the MAC with a keyed hash function. So, the third and fourth messages will have $h_k(...)$ computed over the same messages you see in the protocol, instead of $MAC_k(...)$. Charlie claims that security of this protocol will not be impacted if we are using a CRHF function since still integrity will be preserved (that is, any changes to the nonces will change the output of the hash function). Is Charlie's claim correct? why?

4. For the counter-based RR protocol in slide 8, lecture 9, Alice resets her counter back to 0 after each successful run of this protocol with Bob. What is the impact of this change? Justify your answer.

5. For the 2RT-2PP protocol in slide 10, lecture 9, Roger wants to modify the protocol to have the MAC computed over the *req* and *resp* without encrypting them, i.e., the third message will be $E_{k.e}(req), MAC(3 \parallel A \rightarrow B \parallel N_A \parallel N_B \parallel req)$ and the fourth message will be $E_{k.e}(resp), MAC(4 \parallel A \leftarrow B \parallel N_A \parallel N_B \parallel resp)$. Will that impact the security of the protocol (as compared to the original protocol)? why?

Note: if the scheme is insecure then provide a successful attack against it. If the scheme is secure, just provide a convincing argument (formal security proofs are not required).

Problem 3 [40 points]
Compute the following expressions (please read the note below carefully):

1. $192 \cdot 17^{1700} + 986 \cdot 2024^{56} \mod 37$
2. $576(23023^{1024000} + 365 \cdot 856985^{7202}) \mod 73$
3. $\frac{1436}{8} + \frac{568}{17} + 10785 \mod 101$
4. $2048 - \frac{8}{1436} + \frac{10785}{20 \cdot 17} \mod 99$
5. $10245 \cdot (24 + (345 \cdot 10^{77}(34^{381} + 18976))) \mod 67$
6. $\phi(80) + \phi(2728)$ (First represent each of 80 and 2728 as a product of powers of distinct primes and then compute the Euler's Totient function.)

Note: The goal of this problem is to use the simplification techniques we studied in class. Computing the whole expression (as one shot) using a calculator or some software without showing the simplification steps will be considered a wrong answer. Also, whenever applicable indicate the theorem/lemma/property that allowed the simplification step that you applied. You can use the calculator for intermediate steps that cannot be simplified (for example, multiply numbers or compute a mod operation that cannot be simplified)

Problem 3 [30 points]
This problem is about public key cryptographic primitives.

1. Alice and Bob want to run the DH key exchange protocol for multiplicative cyclic groups. Alice selected the prime $p = 47$ (which satisfies $47 = 2 \cdot 23 + 1$), and the generator $g = 5$. Show an execution of the protocol where Alice chooses the secret key $a = 9$, and Bob chooses the secret key $b = 7$. Show both Alice's computations and Bob's computations in the protocol as well as their outputs.
2. Extend the Diffie-Hellman key exchange protocol to allow four parties (say Alice, Bob, Cameron, and Doug) to exchange a key. So at the end of this protocol, all four parties will establish the same key, say g^{abcd} where c is the secret key that Cameron will choose and d is the secret key that Doug will choose (there is no limit on the number of exchanged messages, so a party may need to send two ore more rounds of messages instead of one as in the 2-party DH key exchange. However, try to minimize the number of sent messages as possible). Consider eavesdropper security as well here.
3. Consider the El-Gamal PKE scheme, and a given a ciphertext (x, y) encrypting some unknown message m (that is, $(x, y) := (g^b, e^b \cdot m)$ where the secret key is a, the public key is $e = g^a$, b is some random integer selected for encryption as we saw in class). Show that given the public key $e = g^a$ and the ciphertext (x, y), it is possible in polynomial time to generate a ciphertext (x', y') encrypting the message km for any desired integer $k \in \mathbb{Z}_p^*$, and such that $x' \neq x$ and $y' \neq y$.