Applied Cryptography: Homework 12

(Deadline: 10:00am, 2020/12/16)

Justify your answers with calculations, proofs, and programs.

1. (15 points, question 10.2, page 412 of the textbook)

   Consider the mutual identification scheme presented in Protocol 10.9. Prove that this scheme is insecure. (In particular, show that Olga can impersonate Bob by means of a certain type of parallel session attack, assuming that Olga has observed a previous session of the scheme between Alice and Bob.)

   Protocol 10.9: INSECURE PUBLIC-KEY MUTUAL AUTHENTICATION

   1. Bob chooses a random challenge, r_1. He also computes $y_1 = \mathbf{sig}_{Bob}(r_1)$ and he sends $\mathbf{Cert}(Bob), r_1$ and y_1 to Alice.
   2. Alice verifies Bob's public key, $\mathbf{ver}_{Bob}$, on the certificate $\mathbf{Cert}(Bob)$. Then she checks that $\mathbf{ver}_{Bob}(r_1, y_1) = true$. If not, then Alice "rejects" and quits. Otherwise, Alice chooses a random challenge, r_2. She also computes $y_2 = \mathbf{sig}_{Alice}(r_1)$ and $y_3 = \mathbf{sig}_{Alice}(r_2)$ and she sends $\mathbf{Cert}(Alice), r_2, y_2$, and y_3 to Bob.
   3. Bob verifies Alice's public key, $\mathbf{ver}_{Alice}$, on the certificate $\mathbf{Cert}(Alice)$. Then he checks that $\mathbf{ver}_{Alice}(r_1, y_2) = true$ and $\mathbf{ver}_{Alice}(r_2, y_3) = true$. If so, then Bob "accepts"; otherwise, Bob "rejects." Bob also computes $y_4 = \mathbf{sig}_{Bob}(r_2)$ and he sends y_4 to Alice.
   4. Alice checks that $\mathbf{ver}_{Bob}(r_2, y_4) = true$. If so, then Alice "accepts"; otherwise, Alice "rejects."

2. (15 points, question 10.5, page 412 of the textbook)

   Prove that Protocol 10.5 and Protocol 10.10 are both insecure if the identity of Alice (Bob, resp.) is omitted from the signature computed by Bob (Alice, resp.).

   Protocol 10.5: PUBLIC-KEY MUTUAL AUTHENTICATION (VERSION 1)

   1. Bob chooses a random challenge, r_1. He sends $\mathbf{Cert}(Bob)$ and r_1 to Alice.
   2. Alice chooses a random challenge, r_2. She also computes $y_1 = \mathbf{sig}_{Alice}(ID(Bob)\|r_1\|r_2)$ and sends $\mathbf{Cert}(Alice), r_2$ and y_1 to Bob.
   3. Bob verifies Alice's public key, $\mathbf{ver}_{Alice}$, on the certificate $\mathbf{Cert}(Alice)$. Then he checks that $\mathbf{ver}_{Alice}(ID(Bob)\|r_1\|r_2, y_1) = true$. If so, then Bob "accepts"; otherwise, Bob "rejects." Bob also computes $y_2 = \mathbf{sig}_{Bob}(ID(Alice)\|r_2)$, and sends y_2 to Alice.
   4. Alice verifies Bob's public key, $\mathbf{ver}_{Bob}$, on the certificate $\mathbf{Cert}(Bob)$. Then she checks that $\mathbf{ver}_{Bob}(ID(Alice)\|r_2, y_2) = true$. If so, then Alice "accepts"; otherwise, Alice "rejects."

Protocol 10.10: PUBLIC-KEY MUTUAL AUTHENTICATION (VERSION 2)

1. Bob chooses a random challenge, r_1. He sends $\mathbf{Cert}(Bob)$ and r_1 to Alice.
2. Alice chooses a random challenge, r_2. She also computes $y_1 = \mathbf{sig}_{Alice}(ID(Bob)\|r_1\|r_2)$ and she sends $\mathbf{Cert}(Alice), r_2$ and y_1 to Bob.
3. Bob verifies Alice's public key, $\mathbf{ver}_{Alice}$, on the certificate $\mathbf{Cert}(Alice)$. Then he checks that $\mathbf{ver}_{Alice}(ID(Bob)\|r_1\|r_2, y_1) = true$. If so, then Bob "accepts"; otherwise, Bob "rejects." Bob also computes $y_2 = \mathbf{sig}_{Bob}(ID(Alice)\|r_2\|r_1)$ and he sends y_2 to Alice.
4. Alice verifies Bob's public key, $\mathbf{ver}_{Bob}$, on the certificate $\mathbf{Cert}(Bob)$. Then she checks that $\mathbf{ver}_{Bob}(ID(Alice)\|r_2|r_1, y_2) = true$. If so, then Alice "accepts"; otherwise, Alice "rejects."

3. (15 points, question 10.6, page 412 of the textbook)

   Consider the following possible identification scheme. Alice possesses a secret key (p, q), where p and q are prime and $p \equiv q \equiv 3 (\bmod 4)$. The value of $n = pq$ will be stored on Alice's certificate. When Alice wants to identify herself to Bob, say, Bob will present Alice with a random quadratic residue modulo n, say x. Then Alice will compute a square root y of x and give it to Bob. Bob then verifies that $y^2 \equiv x (\bmod n)$. Explain why this scheme is insecure.

4. (15 points, question 10.7, page 413 of the textbook)

   Suppose Alice is using the *Schnorr Identification Scheme* where $q = 1201, p = 122503, t = 10$, and $\alpha = 11538$.

   (a) Verify that α has order q in $\mathbb{Z}_p^*$.

   (b) Suppose that Alice's secret exponent is $a = 357$. Compute v.

   (c) Suppose that $k = 868$. Compute γ.

   (d) Suppose that Bob issues the challenge $r = 501$. Compute Alice's response y.

   (e) Perform Bob's calculations to verify y.