CS 798

Assignment 3

due 11:30 AM, Tuesday, November 5

1. Recall that the Computational Diffie-Hellman problem is defined as follows:

   Problem: Computational Diffie-Hellman (CDH)
   Instance: A multiplicative group $(G, \cdot)$, an element $\alpha \in G$ having order n, and two elements $\beta, \gamma \in \langle \alpha \rangle$.
   Question: Find $\delta \in \langle \alpha \rangle$ such that

   $$\log_\alpha \delta \equiv \log_\alpha \beta \times \log_\alpha \gamma \pmod{n}.$$

   (Equivalently, given α^b and α^c, find α^{bc}.)

   The problem that a passive adversary faces in trying to compute a key in the *MTI* protocol is the following:

   Problem: Computational MTI (CMTI)
   Instance: A multiplicative group $(G, \cdot)$, an element $\alpha \in G$ having order n, and four elements $\beta_1, \gamma_1, \beta_2, \gamma_2 \in \langle \alpha \rangle$.
   Question: Find $\delta \in \langle \alpha \rangle$ such that

   $$\log_\alpha \delta \equiv \log_\alpha \beta_1 \times \log_\alpha \gamma_2 + \log_\alpha \beta_2 \times \log_\alpha \gamma_1 \pmod{n}.$$

   (Equivalently, given α^{b_1}, α^{b_2}, and α^{c_1} and α^{c_2}, find $\alpha^{b_1 c_2 + b_2 c_1}$.)

   (a) Prove that CMTI can be solved easily, given an oracle to solve CDH.

   (b) Prove that CDH can be solved easily, given an oracle to solve CMTI.

2. In this question, suppose that $p = 12132217$.

   (a) Factor $p - 1$, and prove that the smallest primitive element modulo p is $\alpha = 5$.

   (b) Suppose $p - 1 \equiv 0 \pmod{q}$ and $\beta \in \mathbb{Z}_p^*$. Let $a_0 = \log_\alpha \beta \bmod q$. Then it is possible to prove that

   $$\beta^{(p-1)/q} \equiv \alpha^{a_0 (p-1)/q} \pmod{p}.$$

   (You are not required to prove this formula.) The formula permits a_0 to be computed in at most q "iterations".

   Using this formula with $q = 167$, apply the method described in class to prove that $(5957975, 512317, 11127721)$ is not a Diffie-Hellman triple in $\mathbb{Z}_p^*$.

3. We describe a secret-key based three-party session key distribution scheme. In this scheme, K_{Alice} is a secret key shared by Alice and the *TA*, and K_{Bob} is a secret key shared by Bob and the *TA*.

   Protocol: SESSION KEY DISTRIBUTION SCHEME

   1. Alice chooses a random number, r_A. Alice sends $ID(Alice)$, $ID(Bob)$ and

      $$y_A = e_{K_{Alice}}(ID(Alice) \parallel ID(Bob) \parallel r_A)$$

      to Bob.

   2. Bob chooses a random number, r_B. Bob sends $ID(Alice)$, $ID(Bob)$, y_A and

      $$y_B = e_{K_{Bob}}(ID(Alice) \parallel ID(Bob) \parallel r_B)$$

      to the *TA*.

   3. The *TA* decrypts y_A using the key K_{Alice} and it decrypts y_B using the key K_{Bob}, thus obtaining r_A and r_B. It chooses a random session key, K, and computes

      $$z_A = e_{K_{Alice}}(r_A \parallel K)$$

      and

      $$z_B = e_{K_{Bob}}(r_B \parallel K).$$

      z_A is sent to Alice and z_B is sent to Bob.

   4. Alice decrypts z_A using the key K_{Alice}, obtaining K; and Bob decrypts z_B using the key K_{Bob}, obtaining K.

   (a) State all consistency checks that should be performed by Alice, Bob and the *TA* during a session of the protocol.

   (b) The protocol is vulnerable to an attack if the *TA* does not perform the necessary consistency checks you described in part (a). Suppose that Oscar replaces $ID(Bob)$ by $ID(Oscar)$, and he also replaces y_B by

   $$y_O = e_{K_{Oscar}}(ID(Alice) \parallel ID(Bob) \parallel r'_B)$$

   in step 2, where r'_B is random. Describe the possible consequences of this attack if the *TA* does not carry out its consistency checks properly.

   (c) In this protocol, encryption is being done to ensure both confidentiality and data integrity. Indicate which pieces of data require encryption for the purposes of confidentiality, and which ones only need to be authenticated. Rewrite the protocol, using MACs for authentication in the appropriate places.

4. We describe a public-key protocol in which Alice chooses a random session key and transmits it to Bob in encrypted form. (A protocol of this type is called a *key transport scheme.*) In this scheme, K_{Bob} is Bob's public encryption key. Alice and Bob also have private signing keys and public verification keys for a signature scheme.

   Protocol: PUBLIC-KEY KEY TRANSPORT SCHEME

   1. Bob chooses a random challenge, r_1. He sends r_1 and $\mathbf{Cert}(Bob)$ to Alice.
   2. Alice verifies Bob's public encryption key, K_{Bob}, on the certificate $\mathbf{Cert}(Bob)$. Then Alice chooses a random session key, K, and computes

      $$z = e_{K_{Bob}}(ID(Alice) \parallel K).$$

      She also computes

      $$y_1 = sig_{Alice}(r_1 \parallel z)$$

      and sends $\mathbf{Cert}(Alice)$, z and y_1 to Bob.
   3. Bob verifies Alice's public verification key, ver_{Alice}, on the certificate $\mathbf{Cert}(Alice)$. Then he checks that

      $$ver_{Alice}(r_1 \parallel z, y_1) = true.$$

      Bob also decrypts z, and verifies that $d_{K_{Bob}}(z)$ has the form $ID(Alice) \parallel K$ for some K. If so, then Bob outputs "accept" and takes K to be the new session key; otherwise, Bob outputs "reject" and quits. Bob also computes

      $$y_2 = sig_{Bob}(z)$$

      and sends y_2 to Alice.
   4. Alice verifies Bob's public verification key, ver_{Bob}, on the certificate $\mathbf{Cert}(Bob)$. Then she checks that

      $$ver_{Bob}(z, y_2) = true.$$

      If so, then Alice outputs "accept"; otherwise, Alice outputs "reject".

   (a) Prove that the above protocol is a secure mutual identification scheme. Analyze an active adversary's probability of successfully deceiving Alice or Bob, given suitable assumptions on the security of the signature scheme.

   (b) What type of key authentication or confirmation is provided by this protocol? Justify your answer briefly.

   Note: You can make an appropriate security assumption regarding the encryption scheme, such as the following: given

   $$z = e_{K_{Bob}}(ID(Alice) \parallel K),$$

   where K is unknown, it is infeasible for Oscar to compute

   $$z' = e_{K_{Bob}}(ID(Oscar) \parallel K)$$

   for the same K. (This property is called *non-malleability.*)

(c) Prove that the protocol is insecure if Alice does not sign z in step 2, by describing two attacks that an active adversary (Oscar) can carry out. Briefly discuss the consequences of these attacks.

Hint: In one attack, Oscar deceives Bob (the initiator of the session); and in the other attack, Oscar deceives Alice.

Notes:

- You can assume that the length of a challenge is the same as the length of an encrypted string (e.g., $|r_1| = |z|$).
- A successful attack is any attack that causes at least one of the honest particpants to "accept" and have false beliefs at the end of a session.