Internet Infrastructure Security (COMP444)
Assignment Two

Each question carries six marks, unless stated otherwise.
** Due on 21 March 2014 **

Rocky K. C. Chang

March 7, 2014

1. `[6 marks]` (RSA) If we select $e = 17$ for RSA, could we use the following values of p, q, and n? (Hint: slide 15 of The RSA Algorithm)

   (a) `[2 marks]` $p = 239$.

   (b) `[2 marks]` $q = 229$.

   (c) `[2 marks]` $n = 211 \times 233$.

2. `[8 marks]` (RSA signature) Alice wants Bob to sign a message m. Assume that Bob's signing is based on RSA. However, she does not want Bob to see the message. Therefore, Alice "blinds" the message by computing $m' = mk^e \mod n$, where k is a random value between 1 and n and $gcd(k, n) = 1$. Alice then presents m' to Bob for his signature. How will Alice obtain Bob's signature on m ($m^d \mod n$) from Bob's signature on m'? Hint: p. 9 of the RSA slides.

3. `[8 marks]` (Forging an RSA signature) Consider that Alice uses RSA to sign digitally. Now Eve would like to obtain Alice's signature on a document m'. To do so, she performs the followings:

   - Choose an arbitrary value x and compute $y = x^e \mod n$, where e is Alice's public exponent.
   - Compute $m = ym' \mod n$.
   - Obtain Alice's signature on m.

   Explain how Eve could obtain Alice signature on m' ($m'^d \mod n$) using the above steps. You may start with the signature of m.

4. `[8 marks]` (A slightly different DH protocol) Another Diffie-Hellman protocol variant is to allow one side to completely determine the shared key. The first few steps are depicted as follows. What should Bob do in the last step in order to derive the same key chosen by Alice?

   (a) Alice randomly selects a large integer x and compute $k = g^x \ mod \ p$.

   (b) Bob randomly selects a large integer y and sends Alice $Y = g^y \ mod \ p$.

(c) Alice sends Bob $X = Y^x \ mod \ p$.

(d) Bob ?

5. [8 marks] (Attacking the Diffie-Hellman exchange) In this question we consider an active attack on the Diffie-Hellman exchange. Before Eve launches this attack, she has to understand certain elementary properties about the multiplicative group modulo prime. In the last question, we have already proved that 1 and $p-1$ are the only elements in $\mathbb{Z}_p^*$ that their multiplicative inverses are themselves.

   (a) [5 marks] Consider that p is a safe prime. That is, $p = 2q+1$, where q is prime, and g is a generator for $\mathbb{Z}_p^*$. Show that $g^q \equiv p-1 (\text{mod } p)$. You may start with the property that $g^{p-1} \text{ mod } p = 1$.

   (b) [3 marks] Now consider the attack. Alice and Bob exchange $g^x \text{ mod } p$ and $g^y \text{ mod } p$. Eve intercepts the messages and changes them to $(g^x)^q \text{ mod } p$ and $(g^y)^q \text{ mod } p$, respectively. What is the result of this attack?

6. [6 marks] (Squares) Referring to the final Diffie-Hellman protocol on slide 21 of Diffie-Hellman (Key Exchange) Protocol, answer the following questions.

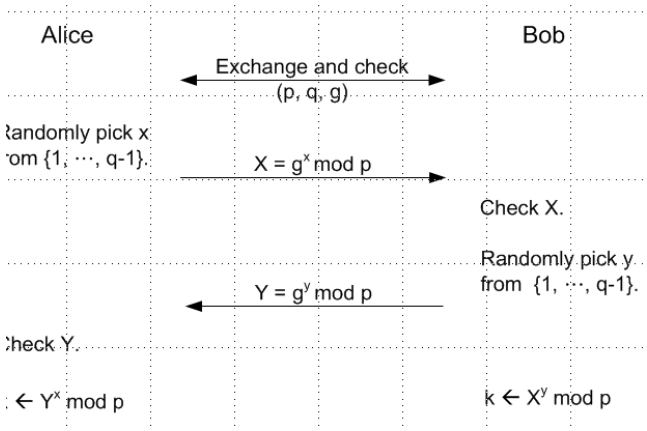

Figure 1: The final Diffie-Hellman protocol.

   (a) [3 marks] Figure 1 shows that Alice and Bob pick their x and y randomly from $\{1, \cdots, q-1\}$. Explain why the set of random numbers is *not* from $\{1, \cdots, p-1\}$.

   (b) [3 marks] The figure also shows that Alice (Bob) needs to check Y (X). What does (s)he need to check?

7. [6 marks] (Mutual authentication) Consider the following mutual authentication protocol where A and B conduct a Diffie-Hellman protocol to come up $K_{AB} = g^{xy} \text{ mod } p$. A and B have agreed on a multiplicative group $\mathbb{Z}_p^*$, and they pick their random numbers x and y from $\mathbb{Z}_p^*$, respectively. Assume that each side can authenticate the other based on digital signatures, and $Sig_A()$ and $Sig_B()$ denote A's and B's signatures, respectively. The signatures are also encrypted by K_{AB}.

1. $A \rightarrow B : A, B, g^x \mod p$

2. $B \rightarrow A : B, A, g^y \mod p, \{Sig_B(g^y \mod p, g^x \mod p)\}_{K_{AB}}$

3. $A \rightarrow B : A, B, \{Sig_A(g^x \mod p, g^y \mod p)\}_{K_{AB}}$

Unfortunately, this protocol is also vulnerable to impersonation attack. Consider that A's first protocol message sent to B is intercepted by an attacker C, and subsequently C could complete the protocol with A successfully. The notation C_B refers to C claiming to be B. Fill in the missing steps below.

1. $A \rightarrow C_B : A, B, g^x \mod p$

1'. $C \rightarrow B :$?

2'. $B \rightarrow C :$?

2. $C_B \rightarrow A : B, A, g^y \mod p, \{Sig_B(g^y \mod p, g^x \mod p)\}_{K_{AB}}$

3. $A \rightarrow C_B : A, B, \{Sig_A(g^x \mod p, g^y \mod p)\}_{K_{AB}}$

8. `[8 marks]` (Authenticated key exchange) Consider the following authenticated key exchange protocol between A and B. Assume that each side can authenticate the other based on digital signatures, and $Sig_A()$ and $Sig_B()$ denote A's and B's signatures, respectively. In step 1, A generates a pair of RSA private and public keys, and sends the public key K_p to B. $E_{K_p}()$ is encryption using the public key K_p, K_{AB} is the session key chosen by B, and N_A is A's nonce.

1. $A \rightarrow B : K_p, N_A, Sig_A(K_p, B)$

2. $B \rightarrow A : E_{K_p}(K_{AB}), Sig_B(h(K_{AB}), A, N_A)$

(a) `[2 marks]` What is the purpose of generating a pair of RSA keys in step 1?

(b) `[2 marks]` What is the purpose of using a hash function $h()$ in step 2?

(c) `[4 marks]` As soon as A receives the message from B, A will destroy the RSA key pair. In this case, will this protocol achieve forward perfect secrecy if A's or B's key for signing is known to an attacker?