IT UNIVERSITY OF COPENHAGEN

Mandatory exercise 1

Course:	Security 1 (fall 2022)
Course code:	BSSECU11KU
Date:	29. september 2022
Author:	Andreas Wachs
Student number:	19167

Solutions

Here I will write about my results and methodology used to solve the three assignments. Commonly for all assignments are the public key provided by Bob in the form of $\{p, g, pk_b\}$ where $p = 6661$, $g = 666$ and $pk_b = 2227$.

In this assignment I've made the attempt to use expressive variable names that have a *readable* (my subjective opinion) name to convey their meaning, such as sk_a for Alice's secret key and pk_b for Bob's public key.

The code

I've implemented solutions to the assignments in the Haskell programming language. You should find the source code provided with this handin. You can run it by installing the Glasgow Haskell Compiler and running the file with the command `$ runhaskell main.hs`.

I have saved an online session of compiling and running the code on a webpage called *Ideone*.You can find it at the following link: `https://ideone.com/HcRbtT`. You can see the output below the source code, on the aforementioned webpage.

Assignment 1

Following the El Gamal cryptoscheme, Bob has provided us with his public key and this enables Alice to begin her part of the scheme. Alice wishes to send the message $m = 2000$.

1. Alice selects a secret key $sk_a = 414$
2. Alice computes a public key $pk_a = g^{sk_a} \textbf{ mod } p = 300$
3. Alice compute the shared key $k = {pk_b}^{sk_a} \textbf{ mod } p = 494$
4. Alice encrypts the message $m' = k \cdot m = 988000$
5. Alice sends Bob her public key along with the encrypted message: $c = (c1, c2) = (pk_a, m') = (300, 988000)$

Alice have now encrypted the message using Bob's public key and sends it to Bob.

Assignment 2

Eve intercepts this message whilst having access to the public key initially sent from Bob. She proceeds to decrypt the message from the nature of poor choice of group and prime in this key exchange.

1. Eve intercepts the message $c = (c_1, c_2) = (300, 988000)$
2. Eve uses the function

$$f(n) = \begin{cases} n & \text{if } g^c \textbf{ mod } p = pk_b \\ f(n+1) & \text{otherwise} \end{cases}$$

to find Bob's private key by brute force: $sk_b = f(0) = 66$

3. Eve now computes the shared key used to encrypt the message: $k = c_1^{sk_b} \textbf{ mod } p = 300^{66} \textbf{ mod } 6661 = 494$
4. Eve is now able to decrypt the message: $\frac{c_2}{k} = \frac{k \cdot m}{k} = m = 2000$

With a weak chosen group and prime for the El Gamal encryption scheme, Eve was able to find Bob's private key from the public information and decrypt the message.

Assignment 3

Mallory also intercepts the message $c = (c_1, c_2)$, but uses a constrained device. She decides to tamper with the message. The goal for Mallory is to triple the numeric value of the message that Bob receives.

1. Mallory creates a tampered message $m' = c_2 \cdot 3 = 6000$
2. Mallory sends Bob the following forged message $c' = (c_1, m') = (300, 6000)$

1. Bob receives the *(forged)* message $c = (c_1, c_2) = (300, 264000)$
2. Bob generates a shared key $k = {c_1}^{sk_b} \textbf{ mod } p = 300^{66} \textbf{ mod } 6661 = 494$
3. Bob now decrypts the message received: $\frac{c_2}{k} = \frac{k \cdot m'}{k} = m' = 6000$

By this, Mallory have successfully tampered with the message sent from Alice. Bob is successful in decrypting the tampered message without any knowledge that it was actually sent from Mallory.