Fundamentals of Cryptography

Homework 5

Dr. Mohammad Dakhilalian

Fall 2023

Theory Part

Question 1

Given an RSA signature scheme with the public key ($n = 9797, e = 131$), show how Oscar can perform an existential forgery attack by providing an example of the parameters of the RSA digital signature scheme.

Question 2

Considering the Elgamal signature scheme, you are given Bob's private key $K_{\text{pr}} = (d) = (67)$ and the corresponding public key $K_{\text{pub}} = (p, \alpha, \beta) = (97, 23, 15)$.

1. Calculate the Elgamal signature (r, s) and the corresponding verification for a message from Bob to Alice with the following messages x and ephemeral keys k_{E}:

   (a) $x = 17$ and $k_E = 31$

   (b) $x = 17$ and $k_E = 49$

   (c) $x = 85$ and $k_E = 77$

2. You receive two alleged messages x_1, x_2 with their corresponding signatures (r_i, s_i) from Bob. Verify whether the messages $(x_1, r_1, s_1) = (22, 37, 33)$ and $(x_2, r_2, s_2) = (82, 13, 65)$ both originate from Bob.

Question 3

Show how DSA can be attacked if the same ephemeral key is used to sign two different messages.

Question 4

We consider three different hash functions which produce outputs of lengths 64, 128, and 160 bits.

1. After how many random inputs do we have a probability of $\epsilon = 0.5$ for a collision?
2. After how many random inputs do we have a probability of $\epsilon = 0.1$ for a collision?

Question 5

1. What is the minimum number of students in a class for at least two students to have the same birthday with a probability greater than 0.5?
2. Find the probability of at least two students having the same birthday as a function of K and N, where N is the number of days in the year and K is the number of students.

Question 6

Draw a block diagram for the following hash functions built from a block cipher $e()$:

1. $e(x_i, x_i \oplus H_{i-1}) \oplus x_i \oplus H_{i-1}$
2. $e(x_i \oplus H_{i-1}, H_{i-1}) \oplus H_{i-1}$

CrypTool Part

Question 7

Answer the following questions concerning the digital signature algorithm;

1. Generate a 2048bit DSA key pair using the CrypTool key generation tool, with your first name, last name, and student ID (as your PIN).
2. Use this key to sign a document of your choice. What does the resulting file consist of?
3. Verify your previous signature using the same key.
4. Make a slight change to the signature and repeat the previous part. Explain what happens.

Programming Part

Question 8

According to Chapter 11, implement the SHA-1 algorithm in your favorite programming language. Your code should receive a string of arbitrary length and compute its SHA-1 hash. Compare your results with built-in SHA-1 implementations.

Optional Part

Question 9 - OpenSSL

Do the following exercises regarding the ECDH cryptosystem;

1. Generate two EC key pairs, using one of the IANA's recommended named curves. Save them in files named "ec_client.key" and "ec_server.key" respectively.
2. Extract the public keys corresponding to the previously generated keys, and save them in files named "client_pub.key" and "server_pub.key".
3. Derive the shared secret value using the pkeyutl command, along with the client's private key, and the server's public key, and name it "secret1".
4. Repeat the previous step but, this time, with the server's private key, and the client's public key, and name the driven file "secret2".
5. How are "secret1" and "secret2" related to each other and why?

To access the list of named curves you might need to visit this link:
`https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8`

If you're interested to learn more about X.509 Public Key Infrastructure Certificate visit this link:
`https://tools.ietf.org/html/rfc5280`