SVS | Exercise 5

Task 1

1. Gegeben ist die Nachricht „VSR“. Berechnen Sie mit Hilfe der ASCII-Tabelle und der Hash-Funktion $f(s) = (\sum_{i=1}^{length(s)} s_i) \ mod \ 7$ den Hash-Wert der Nachricht.
2. Machen Sie sich mit dem GnuPG-Werkzeug[1] vertraut :
   a. Erzeugen Sie den MD5-Hash der Nachricht „VSR“.
   b. Der Hashwert der Datei *bankdaten.txt* ist *„8C E8 26 9E 53 F8 47 57 27 F0 63 41 04 64 DC 3C“*. Prüfen Sie ob die im OPAL eingestellte Kopie der Datei unversehrt ist.
   c. Lassen Sie Ihren Nachbar/Ihre Nachbarin eine der drei Geheimnisse wählen: „fry“, „lila“ oder „bender“. Teilen Sie ihm/ihr anschließend eine zufällige Zahl mit. Lassen Sie Ihren Nachbar/Ihre Nachbarin den MD5-Hash über die Nachricht „Zahl:Geheimnis“ bilden und Ihnen mitteilen. Finden Sie heraus, welches Geheimnis Ihr Nachbar/Ihre Nachbarin gewählt hat.

1. A message „VSR“ is given. Using the ASCII table and the hash function $f(s) = (\sum_{i=1}^{length(s)} s_i) \ mod \ 7$ compute the hash value of the message.
2. Get acquainted with the tool GnuPG[1].
   a. Create a MD5 hash of the message “VSR”.
   b. The hash value of the file *bankdaten.txt* is *„8C E8 26 9E 53 F8 47 57 27 F0 63 41 04 64 DC 3C“.* Check if the copy in OPAL was not manipulated.
   c. Let your neighbor choose one of the three secrets: “fry”, “lila” or “bender”. Afterwards tell him/her a random number. Let him/her build the MD5 hash over the message: “Number:Secret” and tell you the result. Find out which secret your neighbor has chosen.

Task 2

1. Informieren Sie sich über die Caesar-Verschlüsselung. Mit Hilfe des Schlüssels „4“ entschlüsseln Sie die Nachricht „WSQQIV“.
2. Welche Sicherheitsrisiken birgt die Caesar-Chiffre?
3. Entschlüsseln Sie mittels GnuPG (Chiffre: AES, Passwort: *tu-chemnitz*) die Datei *image.png.gpg*

1. Read about the Caesar cipher. Using the key “4” decrypt the message “WSQQIV”.
2. Which security risks are imposed by the Caesar cipher?
3. Using GnuPG decrypt the file image.png.gpg (Cipher: AES, Password: tu-chemnitz)

[1] Z.B. hier: http://www.gnupg.org/gph/en/manual/book1.html

Task 3

1. Betrachten Sie die Ver- und Entschlüsselung mittels RSA[2]:
   a. Ihr Kommunikationspartner hat Ihnen seinen öffentlichen Schlüssel (RSA) mitgeteilt: PUBKEY = (e = 7, N = 77). Verschlüsseln Sie an ihn die Nachricht „DE“, indem Sie Buchstaben ihren Ordnungsnummern im Alphabet gleichsetzen.
   b. Entschlüsseln Sie den Code aus der Teilaufgabe a mittels dem privaten Schlüssel PRIVKEY = (d = 43, N = 77).
2. Erzeugen Sie mit dem Werkzeug GnuPG ein RSA-Schlüsselpaar. Tauschen Sie mit Ihrem Nachbar/Ihrer Nachbarin die öffentlichen Schlüssel aus:
   a. Erzeugen Sie im OPAL-Ordner „Schlüsseldatenbank“ einen Ordner mit Ihrem URZ Nutzerkürzel.
   b. Laden Sie Ihren öffentlichen Schlüssel in den Ordner hoch.
3. Schreiben Sie eine Nachricht an Ihren Nachbar/Ihre Nachbarin, verschlüsseln Sie diese mit dem öffentlichen Schlüssel Ihres Nachbars/Ihrer Nachbarin und laden Sie die verschlüsselte Datei in den OPAL-Ordner Ihres Nachbars/Ihrer Nachbarin hoch.
4. Entschlüsseln Sie die erhaltene Datei mittels Ihres privaten Schlüssels.

1. Consider the RSA[2] encryption and decryption:
   a. Your communication partner passed you a public key PUBKEY = (e = 7, N = 77). Encrypt the message “DE” using this public key. Use positions of letters in alphabet as codes.
   b. Decrypt the message from subtask a using the private key PRIVKEY = (d = 43, N = 77).
2. Using the GnuPG tool create a RSA key pair. Exchange public keys with your neighbor:
   a. Create a folder with your URZ username in the “Schlüsseldatenbank” folder of OPAL.
   b. Upload your public key to the folder of your neighbor.
3. Create a message to your neighbor, encrypt it using his / her public key and upload the encrypted file to his folder in OPAL.
4. Decrypt the message using your private key.

Task 4

1. Informieren Sie sich über die Signaturbildung mittels RSA.
   a. Signieren Sie die Nachricht „DE“ mittels ihres privaten Schlüssels (d* = 27, N* = 55).
   b. Ihr Kommunikationspartner kennt Ihren öffentlichen Schlüssel - (e* = 3, N* = 55). Wie überprüft er Ihre Signatur?
2. Signieren Sie die Nachricht aus der Aufgabe 3.3. Verändern Sie **optional** den Inhalt der Nachricht. Laden Sie die Datei und die Signatur in den OPAL-Ordner Ihres Nachbars/Ihrer Nachbarin hoch. Lassen Sie Ihren Nachbar/Ihre Nachbarin prüfen, ob die Nachricht der Signatur entspricht.

1. Inform yourself about building signatures using RSA.
   a. Sign the message “DE” using your private key (d* = 27, N* = 55)
   b. Your communication partner knows your public key - (e* = 3, N* = 55). How can he verify your signature?
2. Sign the message from task 3.3. If you want you can change the message’s content. Upload both the message and the signature into the OPAL folder of your neighbor. Let him/her check if the message corresponds to the signature.

---

[2] RSA-Verschlüsselung: $c = f(m) = m^e \ mod \ N$
RSA-Entschlüsselung: $f^{-1}(c) = c^d \ mod \ N$

Homework

1. Denken Sie sich einen geheimen Schlüssel aus (im Folgenden als Sitzungsschlüssel genannt). Verschlüsseln Sie anschließend damit eine Nachricht (eine Datei) an Ihren Nachbar / Ihre Nachbarin.
2. Signieren Sie den Sitzungsschlüssel und verschlüsseln Sie ihn sowie seine Signatur mit dem öffentlichen Schlüssel Ihres Nachbars / Ihrer Nachbarin. Laden Sie die verschlüsselten Schlüssel und Signatur in den Ordner Ihres Nachbars / Ihrer Nachbarin hoch.
3. Lassen Sie Ihren Nachbar / Ihre Nachbarin die ursprüngliche Nachricht entschlüsseln.

1. Choose yourself some secret phrase (named session key in the following). Using the session key encrypt a message (a file) to your neighbor.
2. Sign the session key, encrypt it and its signature using the public key of your neighbor. Upload the encrypted files to the his / her OPAL folder.
3. Let your neighbor decrypt the message.