Praktikum IT-Sicherheit

- Versuchshandbuch -

IT-Sicherheit

Aufgaben

Kryptografie I

In diesem Versuch werden Sie verschiedene Verschlüsselungsverfahren und deren Funktionsweise kennenlernen und einsetzen. Anhand von Beispielen werden Sie einige Einsatzmöglichkeiten der Kryptographie nachstellen.

B.Sc. AI, WI
M.Sc. AI
M.Sc. EB

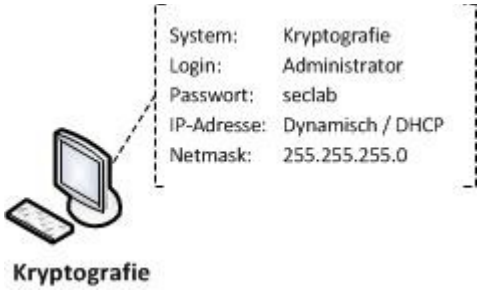
Einleitung

Kryptografische Verfahren werden in rechnerbasierten Kommunikationsnetzen nicht nur zur Gewährleistung von Vertraulichkeit eingesetzt, sondern auch zum Schutz vor Datenmanipulation, nicht autorisierter Dienstnutzung und Abstreitbarkeit durchgeführter Aktivitäten. Mit Hilfe von CrypTool werden Einblicke sowohl in historische als auch aktuelle Verschlüsselungsverfahren gewährt, Hashverfahren vorgestellt und die Verwendung digitaler Signaturen demonstriert. Sicherheitsprobleme einzelner kryptographischer Systeme werden herausgestellt.

Zugangsdaten

- System: Windows XP
- Benutzer: Administrator
- Passwort: seclab

Netzwerkplan



Aufgabe 1: Historische Verschlüsselungsverfahren

a) Welches ist das wohl bekannteste historische Verschlüsselungsverfahren? Beschreiben Sie in wenigen Worten dessen Funktionsweise.

.....

.....

.....

.....

b) Wo liegt die Schwäche dieses Verfahrens ?

.....

.....

.....

.....

c) Entschlüsseln und beantworten Sie die folgende, im Caesar-Verfahren verschlüsselte Frage. Verwenden Sie dazu das Programm „CrypTool".

„Ami jyroxmsrmivx hew Zivjelvir zsr Zmkrivi dyv Zivwglpyiwwipyrk zsr Reglvmglxir? Ivpeiyxivr wmi hmi Yrxivwglmihi dyq Zivjelvir zsr Geiwev yrh jyilvir wmi eyw, aevyq hew Zivjelvir zsr Zmkrivi fiwwiv mwx."

Hinweis : Cryptool → Analyse → Symmetrische Verschlüsselung (klassisch) → Cyphertext-only → Caesar

.....

.....

.....

.....

.....

.....

.....

d) Welchen Schlüssel verwendet die folgende, im Vignere-Verfahren verschlüsselte Nachricht? Folgen sie den Anweisungen der Nachricht und beantworten sie eventuelle Fragen.

„Niydtuillr Oxaijoegtwjl, auk lhfmz kmui qy Bmnrmdk Zlvnmnvlr dqxwjltgkwzitfk Rhgpdogox mzzwjltgkwzitf. Biywconiu wqq tyu iqzk obizlkvl Rionvpgpf sma hmy mplmktkr Zgpxaizwmx fy cizeilsymeyisr czj qpx Kdetaswx fy lrbeilsymeyisr. Emxyt izyoxaitf Ivftbaup kiv rgpzgpqt Wjltgkwzit?"

.....

.....

.....

.....

.....

e) Was ist ein One-Time-Pad?

.....

.....

.....

.....

.....

Aufgabe 2: Faktorisieren

a) Was versteht man unter dem Faktorisieren eines RSA-Schlüssels (… Faktorisieren des RSA-Moduls N) ?

.....

.....

.....

.....

.....

.....

b) Schätzen Sie, in welcher Zeit ein RSA-Schlüssel (64 Bit und 128 Bit) in seine Primfaktoren zerlegt werden kann. Warum ist eine solche Schätzung schwierig?

.....

.....

.....

.....

c) Vergleichen Sie ihre Schätzungen mit den Zeiten, die CrypTool für die Faktorisierung benötigt.

- Erzeugen einer 128 Bit Zahl
  - Wählen Sie im Menü *Einzelverfahren → RSA-Kryptosystem → RSA-Demo*
  - Klicken Sie auf den Button *Primzahlen generieren*
  - Wählen Sie für p und q die *Untergrenze 2^63,* die *Obergrenze 2^64* und klicken Sie anschließend zuerst auf *Primzahlen generieren* und danach auf *Primzahlen übernehmen*
  - Im Feld *RSA-Modul N* befindet sich nun der öffentliche Teil des Schlüssels, den Sie in die Zwischenablage kopieren
- Faktorisieren einer 128 Bit Zahl
  - Wählen Sie im Menü *Einzelverfahren → RSA-Kryptosystem → Faktorisieren einer Zahl*
  - Fügen Sie die 128 Bit Zahl in das Eingabefeld ein und klicken Sie auf *Weiter*
  - Nach Beendigung der Faktorisierung, klicken Sie auf *Details*

Aufgabe 3: Der Dialog der Schwestern

a) Lösen Sie die Aufgabe aus der Kurzgeschichte „Der Dialog der Schwestern". Nennen Sie sowohl das Lösungswort, als auch die benötigen Zwischenergebnisse.

.....

.....

.....

.....

.....

.....

.....

.....

Zur Erinnerung:

- Öffentlicher Schlüssel: 681, 151
- Verschlüsselter Text: 172, 1734, 315, 641, 372, 3491, 360, 387, 586, 602, 2358
- Vorgehensweise:
  - Faktorisieren Sie zuerst die Zahl 681
  - Rufen Sie dann über das Menü *RSA-Demo* auf
  - Geben Sie die ermittelten Primfaktoren, den zweiten Teil des öffentlichen Schlüssels (e = 151) und den verschlüsselten Text ein. Wählen Sie für die Art des Textes „Eingabe als Zahlen"
  - Klicken Sie auf *Optionen für Alphabet und Zahlensystem* und wählen Sie die RSA-Variante „Dialog der Schwestern"

    Achtung: Das Alphabet der Schwestern besitzt lediglich 26 Zeichen. Im vorgegebenen Alphabet befindet sich zusätzlich ein Leerzeichen, das Sie entfernen müssen.

Das Problem kann auch rechnerisch gelöst werden. Siehe dazu
http://www.computerjockey.de/stories/file_dialog.html

Aufgabe 4: RSA-Schlüsselpaar erzeugen

a) Erzeugen Sie mit Hilfe von „CrypTool" ein *RSA-Schlüsselpaar*.

- Wählen Sie im Menü *Digitale Signaturen/PKI → PKI → Schlüssel erzeugen/importieren*
- Wählen Sie das RSA-Verfahren mit einer Bitlänge von 1024
- Tragen Sie Ihre Benutzerdaten und eine PIN ein
- Klicken Sie auf den Button *Neues Schlüsselpaar erzeugen*
- Nach der Erzeugung des Schlüssels klicken Sie auf *Übernehmen*, um den Schlüssel zu speichern

b) Signieren Sie nun ein Dokument mit Ihrem Schlüssel.

- Erzeugen Sie zunächst ein neues Dokument mit beliebigem Inhalt auf dem Desktop oder direkt in CrypTool
- Öffnen Sie die Signaturdemo (*Einzelverfahren → RSA-Kryptosystem → Signaturdemo*)
- Im Fenster „Schrittweise Signaturerzeugung" sehen Sie nun die einzelnen Schritte, die zur Erzeugung der Signatur des Dokuments durchgeführt werden müssen
- Falls Sie ein Dokument in CrypTool erzeugt haben, wurde dieses bereits geladen. Andernfalls können Sie ein Dokument wählen, indem Sie auf „Dokument öffnen" klicken
- Wählen Sie anschließend die *Hashfunktion SHA1* und klicken Sie danach auf *Hashwert berechnen*
- Klicken Sie nun auf *Zertifikat bereitstellen → Zertifikat/Schlüssel importieren* und wählen Sie den zuvor erzeugten Schlüssel aus
- Verschlüsseln Sie jetzt den zuvor berechneten Hashwert mit dem geladenen Schlüssel
- Abschließend können Sie die Signatur des Dokumentes generieren und speichern

c) Signieren Sie ein weiteres Dokument mit anderem Inhalt und vergleichen Sie die beiden Signaturen. Gibt es Unterschiede? Warum? Beschreiben Sie kurz wie die Erzeugung einer Signatur abläuft.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....