Kristof Van Laerhoven
Thomas Janson

Freiburg, den 8. Mai 2015
Besprechung 15. Mai 2015

Übungen zur Vorlesung

Systeme II / Rechnernetze

Sommer 2015

Blatt 2 (15 Punkte)

AUFGABE 1: 4 Punkte

1. Nennen Sie den grundlegenden Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren und die Vor- und Nachteile.

2. Nennen Sie je zwei Beispiele für Anwendungen, die symmetrische oder asymmetrische Verschlüsselungsverfahren benutzen.

AUFGABE 2: 6 Punkte

Eamad oyeex ozma nyi il
Eamad oyeex kas nyi gyte
Eamad oyeex die xdyieg xeg gavads nyi
Eamad oyeex qxba nyi fdn
Eamad oyeex vxn oyygjna
Eamad oyeex sakk x kza xeg uids nyi

Sie fangen einen chiffrierten Text ab, zu dem Sie den Schlüssel nicht kennen. Aus Erfahrung wissen Sie, dass die Kommunikationspartner nur ein symmetrisches Verschlüsselungsverfahren mit einem monoalphabetischem Schlüssel verwenden. Ferner kennen sie die Buchstabenhäufigkeitsverteilung im Ursprungstext:

Buchstabe	Prozentualer Anteil im Text	Buchstabe	Prozentualer Anteil im Text
N	0,17	G,Y	0,06
E	0,14	V	0,05
O	0,11	D	0,04
A	0,09	L,T	0,03
R	0,08	I, S, B, C, H, K, M, P, W	0,01
U	0,07	F, Q, X, Z	0

Entschlüsseln Sie den Text. Um was für eine Art von Angriff handelte es sich und welche anderen Arten von Angriffen gibt es noch?

AUFGABE 3: 5 Punkte

Ein Server benutzt zur verschlüsselten Kommunikation das RSA-Verfahren mit folgendem Public-Key: $(N, e) = (1739, 1001)$

1. Wieso würde man solch einen Public-Key in der Realität nicht einsetzen?

2. Faktorisieren Sie N und errechnen Sie davon ausgehend dann d.

3. Sie haben folgende Daten bei einer Kommunikation zwischen dem Server und einem Client mitgeschnitten:
   $1272 \quad 666 \quad 666 \quad 1080 \quad 1272 \quad 1341 \quad 470 \quad 437 \quad 964 \quad 1258 \quad 59 \quad 1382 \quad 1460$
   Entschlüsseln Sie die Daten.[1]

4. Wie groß dürfen die zu verschlüsselnden Zahlen in diesem Fall maximal sein? Was passiert, wenn eine Zahl größer ist?

[1] TIPP: Die Daten sind in ASCII kodiert. Jede Zahl steht für ein Zeichen.