Übung zur Vorlesung „Sicherheit“

Florian Böhl
florian.boehl@kit.edu

Sicherheit – Literatur zur Vorlesung

Jonathan Katz, Yehuda Lindell. *Introduction to Modern Cryptography*. ISBN 1-584-88551-3.
`http://www.cs.umd.edu/~jkatz/imc.html`

Ross Andersson. *Security Engineering*. ISBN 0-470-06852-3.
`http://www.cl.cam.ac.uk/~rja14/book.html`

Skript auf der Vorlesungs-Webseite.

Organisatorisches

- Ü-Eier für Korrekturen am Skript
- Kummerkasten auf Vorlesungs-Webseite
- Übungsblätter zur Korrektur abgeben

Ein paar Worte zu Übung und Übungsblättern

- Übungsblätter freiwillig
- Abgabe der Übungsblätter möglich
- Übung für Fragen und Diskussionen

Werbung

IEEE Student Branch Karlsruhe präsentiert...

1st IEEE

Signal Intelligence Challenge

"THE SPECTRUM MENACE"

00110010111011--WER FINDET DIE VERSTECKTEN NACHRICHTEN?

Informationsveranstaltung am 5. Mai

`http://www-ieee.etec.uni-karlsruhe.de/`

Fragen?

Restliche Agenda für heute

- Aufgaben besprechen
  - Vigenère
  - One-Time-Pad
  - Verwendung von Blockchiffren
- Demo: Verwundbarkeit von CBC

Sicherheit – Übungsblatt 1

Aufgabe 1. Gegeben ist der folgende Chiffretext. Ermitteln Sie den dazugehörigen Klartext. (Hinweis: Als Verschlüsselungsmechanismus wurde das Vigenère-Verfahren benutzt.)

```
MZMTELFMPLWUFEWXTZPCJDQPBVUKSIEEQDIMIIDRLQNTPWFBZNYNTTQLMAFAGQADDYXOPLIDIWYXFIN
ISZBSCZUOPLIDMNGTTMCCEDTTCVMBEYGWACCPUMOMRWVZUPQLRCSRBSCTXITLXQFEGSDCDCSRICCGAO
YGDMJWCAAZOYWMSPWOMATQOUAXCXTWOFEPVZQYOPOCTQVOCROQPQOMATQOUELQXTMQGVEBEMTGJWGWT
IYYGOWFLXANEFIMBEYGWJFRMFQDAPQICRLMBEFIDMHCVQWEFIDAHFSIMCCEIICCSRQEGRQQRFXQMYDM
RBJDSGZNFEDTPQFMJMYKQELQKAIOCHUVEMFDMLIMZOEFIHQRCRQZPAMBPPPATMYHSTVSYPXJCMGWBSU
EUBPQWGJXGXFMOYRQENGTTMCRSFPPHSGZYYPANEFIEWNGIFGZDXTMLPXEESCRNIMZESMDFSIMORLMBE
FAMQECWOQAFIDELQIEAPLXUIWJCVCDREZWEFIDZPAVQIEGSZWQRLQDTEIZMCCGUXSCVFPHYMFMDALMT
WCRSMOZENJLEIFWMPIMSSGWOQAFIDMYASPMORAUKPUMFPVCCEWQBMRNPPIZBWCRSBSZENJLEIECNAIQ
LPBMZLPAVKXEGRSIDYQBTPULUKSRYDVPBSGBEMFQBSCTAMXRLQDTQMAVZDWUVMWEXNCCHFMYLCEWYCR
OZJNXQLLAGAZOGRSBZRLQSPWAAZOCQUTJRLQNTPWFVLKIANECRZGDMREETDINIMZESMYCZQZPVTXITL
IPBSCQQBSMHTMFQIPAESHUMDMJNIMZESMDLSFMDPIHMLJXTIEFITIOSWQLEFIYMEFSPTLRIDXFZPUAS
CHNGVYWUAVGEZLDSKSMDRXTIEFITIOZIQVFQMZOEFIYMEFSPIDCEDTJYWQQRFXQMYDSGZEWWUF
```

Sicherheit – Übungsblatt 1 – Aufgabe 1

Lösungsvorschlag zu Aufgabe 1. Beim Brechen von Vigènere-Chiffraten gehen wir wie folgt vor:

- Wir raten die Länge ℓ des Schlüssels $K = K_1 K_2 \dots K_\ell$ (oder wir nutzen die Kasiski-, Friedmann- oder die Autokorrelations-Methode).

Sicherheit – Übungsblatt 1 – Aufgabe 1

Lösungsvorschlag zu Aufgabe 1. Beim Brechen von Vigènere-Chiffraten gehen wir wie folgt vor:

- Wir raten die Länge ℓ des Schlüssels $K = K_1 K_2 \ldots K_\ell$ (oder wir nutzen die Kasiski-, Friedmann- oder die Autokorrelations-Methode).
- Wir teilen das Chiffrat in ℓ Teile auf, z.B. für $\ell = 5$:

  MZMTELFMPLWUFEWXTZPCJDQPBVUKSIEE...

  MZMTELFMPLWUFEWXTZPCJDQPBVUKSIEE...

  ...

  MZMTELFMPLWUFEWXTZPCJDQPBVUKSIEE...

Sicherheit – Übungsblatt 1 – Aufgabe 1

Lösungsvorschlag zu Aufgabe 1. Beim Brechen von Vigènere-Chiffraten gehen wir wie folgt vor:

- Wir raten die Länge ℓ des Schlüssels $K = K_1 K_2 \ldots K_\ell$ (oder wir nutzen die Kasiski-, Friedmann- oder die Autokorrelations-Methode).
- Wir teilen das Chiffrat in ℓ Teile auf, z.B. für $\ell = 5$:

  MZMTELFMPLWUFEWXTZPCJDQPBVUKSIEE...

  MZMTELFMPLWUFEWXTZPCJDQPBVUKSIEE...

  ...

  MZMTELFMPLWUFEWXTZPCJDQPBVUKSIEE...
- Wir führen eine Frequenzanalyse auf jedem Teiltext durch.

```
A: **********************************
B: ******
C: ***********
D: ******************
E: **************************************************
F: *********
G: ********
H: ************************
I: ****************************
J: *
K: ***
L: ****************
M: **********
N: ***************************
O: *********************************
P: ********
Q:
R: ************************
S: ***************************
T: ************************************
U: ************
V: ****
W: *********
X: *
Y: ********
Z:
```

Erwartete Buchstabenhäufigkeit im Englischen (Quelle: Wikipedia).

```
A: **************************
B: ********
C: ************
D: ********************
E: ************************************************************************
F: *******
G: ************
H: ********************
I: ******************************
J: *
K: *****
L: ***************
M: **********
N: ****************************************
O: **********
P: ***
Q:
R: ****************************
S: ******************************
T: ************************
U: ******************
V: ***
W: ********
X:
Y:
Z: *****
```

Erwartete Buchstabenhäufigkeit im Deutschen (Quelle: Wikipedia).

Sicherheit – Übungsblatt 1 – Aufgabe 1

- Wir vergleichen die natürliche Alphabetverteilung mit der Verteilung, die aus der Frequenzanalyse hervorging.

Die Buchstabenverteilung für den obigen Chiffretext und ersten Teiltext, der mit K_1 verschlüsselt wurde, sieht wie folgt aus:

A: **********
B:
C: ******
D: **
E: **********
F: ******
G: **********
H: **********
I: **********
J: ****
K: ******
L: **********
M: **********
N:
O: ********
P: **********
Q: ******
R: **********
S: **********
T: **********
U:
V: **********
W: **********
X: **********
Y: ********
Z: ****

Sicherheit – Übungsblatt 1 – Aufgabe 1

- Vermutlich wurde $\mathtt{E}$ (der häufigste Buchstabe im natürlichen Alphabet) $\mathtt{I}$ abgebildet. Damit ist $\mathtt{I} - \mathtt{E} = \mathtt{E}$ der wahrscheinlichste Kandidat für K_1 ergeben.
- Wir folgen dieser Strategie für K_2 bis K_5 und erhalten einen Schlüsselkandidaten.
- Falls eine Entschlüsselung mit $K_1 = \mathtt{E}$ kein sinnvolles Ergebnis liefert, reicht es in der Regel, an problematischen Schlüsselstellen zum nächst häufigsten Buchstaben überzugehen. Für K_1 wäre das beispielsweise $\mathtt{S} - \mathtt{E} = \mathtt{O}$.

Sicherheit – Übungsblatt 1 – Aufgabe 1

Demo in der Übung (siehe vigenere.py).

Sicherheit – Übungsblatt 1 – Aufgabe 1

Der geheime Schlüssel lautet `EMILY`. Damit ergibt sich (unter Hinzufügen von Groß-/Kleinschreibung, Leer- und Satzzeichen und Ersetzen von Zahlwörtern,) der Klartext:

```
In 1863 Friedrich Kasiski was the first to publish a successful general
attack on the Vigenère cipher. Earlier attacks relied on knowledge of
the plaintext, or use of a recognizable word as a key. Kasiski's method
had no such dependencies. Kasiski was the first to publish an account of
the attack, but it is clear that there were others who were aware of it.
In 1854, Charles Babbage was goaded into breaking the Vigenère cipher
when John Hall Brock Thwaites submitted a 'new' cipher to the Journal of
the Society of the Arts....
```

Sicherheit – Übungsblatt 1 – Aufgabe 1

Fazit:

- Wir wissen, wie die Vigenère-Chiffre funktioniert und dass sie sich leicht brechen lässt.
- Eine gute Chiffre versteckt Verteilungen auf der Eingabe.
- „Emily“ist kein geeignetes Passwort :)

Fragen?

Sicherheit – Übungsblatt 1 – Aufgabe 2

Das Wiederverwenden eines Schlüssels K im One-Time-Pad-Verfahren birgt Angriffsmöglichkeiten. Schreiben Sie ein Programm (beispielsweise ein Pythonskript), das zwei im WAVE-Format kodierte Dateien M_1, M_2 mithilfe des One-Time-Pad-Verfahrens verschlüsselt und dabei denselben Schlüssel K verwendet. Was passiert, wenn Sie die beiden Chiffrate XOR-verknüpfen? (Hinweis: Falls Sie eine XOR-verknüpfte Datei in einem Mediaplayer abspielen möchten, benötigen Sie einen korrekten WAVE-Dateiformat-Header. Wie könnte dieser aussehen, wenn Sie die ursprünglichen im WAVE-Format gespeicherten Klartexte nicht kennen?)

Sicherheit – Übungsblatt 1 – Aufgabe 2

Lösungsvorschlag. Unten gegeben ist ein Pythonskript, dass zwei im WAVE-Dateiformat geladene Dateien M_1, M_2 mit demselben Schlüssel K verschlüsselt. Somit erhalten wir $C_1 := M_1 \oplus K$ und $C_2 := M_2 \oplus K$. Anschließend werden beide Chiffrate XOR-verknüpft; das heißt, wir erhalten $C' := C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K) = M_1 \oplus M_2$. Im letzten Schritt wird eine gültige WAVE-Datei aus C' erstellt. Ausgehend davon können diese Header-Werte angepasst und weitere, in Abhängigkeit stehende Werte berechnet werden. Ein mögliches Pythonskript könnte wie folgt aussehen:

Sicherheit – Übungsblatt 1 – Aufgabe 2

Eventuell muss ein wenig mit den Header-Werten experimentiert werden, da wir nicht davon ausgehen können, dass wir den Klartext – und somit die Header-Informationen – kennen. Wir könnten als Ansatzpunkt annehmen, dass die Daten

- aus einer Quelle stammen,
- im PCM-Verfahren moduliert sind,
- eine Abtastrate von 44100 Hz haben und
- 2 Kanäle Stereo bereithalten.)

Ausgehend davon können diese Header-Werte angepasst und weitere, in Abhängigkeit stehende Werte berechnet werden. Ein mögliches Pythonskript könnte wie folgt aussehen:

Sicherheit – Übungsblatt 1 – Aufgabe 2

Demo

Sicherheit – Übungsblatt 1 – Aufgabe 2

Fazit:

- Theoretisch ist das One-Time-Pad perfekt sicher – man darf allerdings keinesfalls den gleichen Schlüssel zwei Mal verwenden.

- Das One-Time-Pad ist hochgradig verwundbar (malleable).

Fragen?

Sicherheit – Übungsblatt 2 – Aufgabe 3

Wir wissen, dass die Blockchiffre $(\mathrm{E}, \mathrm{D}) : \{0,1\}^8 \times \{0,1\}^4 \to \{0,1\}^4$ bei Eingabe eines festen Schlüssels K_0 eine Eingabe M wie folgt auf eine Ausgabe $C := \mathrm{E}(K_0, M)$ abbildet:

M	0000	0001	0010	0011	0100	0101	0110	0111
C	0111	1111	1110	0001	1101	0101	1010	0011

M	1000	1001	1010	1011	1100	1101	1110	1111
C	1000	0010	1001	0100	1011	0000	1100	0110

Verschlüsseln Sie die Klartexte $M_1 = 0100\ 1011\ 0100\ 0001$ und $M_2 = 0100\ 1101\ 0100\ 0001$ unter K_0 in den Betriebsmodi Electronic Code Book (ECB), Cipher Block Chaining (CBC) und Counter Mode (CTR). Worauf sollte bei der Wahl eines Initialisierungsvektors IV in den einzelnen Modi, falls vonnöten, geachtet werden?

Sicherheit – Verwundbarkeit von CBC

heise Security

News | Hintergrund | Erste Hilfe

Security > Hintergrund > Erfolgreicher Angriff auf Linux-Verschlüsselung

Erfolgreicher Angriff auf Linux-Verschlüsselung

23.12.2013

Linux Unified Key Setup (LUKS) ist das Standardverfahren für die Komplettverschlüsselung der Festplatte unter Linux; viele Systeme, darunter Ubuntu 12.04 LTS, setzen dabei LUKS im CBC-Modus ein. Jakob Lell demonstriert, dass diese Kombination anfällig für das Einschleusen einer Hintertür ist. Dabei manipuliert er nicht etwa den unverschlüsselten Boot-Sektor (was der allgemein bekannten Evil Maid Attack entspräche) sondern den verschlüsselten Cipher-Text. Lell nutzt dabei das bereits seit längerem bekannte Problem, dass man bei CBC einzelne Blöcke ganz gezielt manipulieren kann. Einzige Voraussetzung für den Angriff ist, dass man die Position einer Datei exakt kennt.

Das eigentliche „Problem“ ist schon seit 2005 bekannt...
und das schauen wir uns nun an.

Sicherheit – Verwundbarkeit von CBC

Fazit:

- CBC ist relativ einfach verwundbar
- Immer wichtig: Ist der Angreifer aktiv oder passiv?

  Aktuelles Thema in der VL: Was bedeutet Sicherheit gegen passive Angreifer?

Fragen?

Information

- Nächste Vorlesung: Mo, 27.04.
- Nächstes Übungsblatt: Mo, 27.04.
- Nächste Übung: Do, 08.05.