

Security

Sommersemester 2021

(LV 4121 und 4241)

10. Aufgabenblatt

Das folgende Aufgabenblatt beschäftigt sich zunächst mit der Anwendung einer Vigenère-Chiffre. Im Anschluss daran schätzen wir die erforderliche Rechenzeit für einen Brute-Force-Angriff auf einen Blockalgorithmus ab. Schließlich analysieren wir einen One-Time-Pad und stellen dabei einige grundsätzliche Überlegungen an.

Aufgabe 10.1

- a) Dechiffrieren Sie die nachfolgenden Geheimtexte von denen Sie wissen, dass eine Verschiebechiffre (Vigenère-Chiffre, 1586) mit dem Schlüssel $K = 5$ benutzt wurde. Benutzen Sie hierzu ggf. ein selbstentwickeltes Rechnerprogramm!
- i) UTQDFQUMFGJYNXHM
 - ii) FXDRRJYW NXHM
 - iii) NSAJWYNJW GFW
- b) Ist die folgende Aussage „Es ist entscheidend, dass an jeder Stelle des Kryptogramms der Schlüssel eindeutig den Klartextbuchstaben zu jedem Geheimtextbuchstaben festlegt“ richtig?

Aufgabe 10.2

Berechnen Sie die Zeit für das Knacken des 1024-Bit-Schlüssels einer 1024-Bit-Blockchiffre mit einem Brute-Force-Angriff unter der Annahme, dass Sie einen Block von 1024 Bit im Klartext und im Chiffretext vorliegen haben. Nehmen Sie ferner an, dass Sie Zugriff auf einen Rechner haben, der pro Sekunde 1 Megabit verschlüsseln kann.

Aufgabe 10.3

Beim One-Time-Pad darf der Schlüsselstrom nicht wiederholt oder für eine andere Nachricht verwendet werden, da sonst durch Korrelation der beiden Chiffretexte eventuell die Chiffre gebrochen werden kann. Diesen Sachverhalt verdeutlichen wir beispielhaft an einer Vernam-Chiffre, die ja bekanntlich einer Vigenère-Chiffre mit einem Klar- und Chiffrealphabet von $\{0, 1\}$ entspricht. Dabei seien $P = p_1 p_2 \dots$ ein Klartext und $K = k_1 k_2 \dots$ ein Schlüssel mit $p_i, k_i \in \{0, 1\}$, $i = 1, 2, \dots$. Dann setzen wir $C = E_K(P) = c_1 c_2 \dots$ mit $c_i = p_i \oplus k_i$, $i = 1, 2, \dots$, wobei \oplus das exklusive Oder ist.

Ein Klartext P werde nun mit dem Schlüssel K chiffriert und ausgesendet. Durch einen Angreifer werde nun dieser Chiffretext mit einem mit dem gleichen Schlüssel erzeugten Chiffretext überlagert.

- Auf welche Weise (formale Herleitung) lässt sich mit Hilfe des korrelierten Chiffretextes der Klartext P rekonstruieren?
- Es sei $C' = 0111\ 0101$ der korrelierte Chiffretext und $P' = 0010\ 1001$ der dem Angreifer bekannte Klartext. Wie lautet der ursprünglich ausgesendete Klartext P?
- Wie ermittelt der Angreifer hieraus den Schlüssel K?

Aufgabe 10.4

Sender und Empfänger eines Kommunikationskanals stützen den Datenaustausch auf ein Rabin-Kryptosystem ab.

- Der Sender verschlüsselt den Klartext $T = 11$ mithilfe des Rabin-Moduls $n = 57$. Wie lautet der zugehörige Ciphertext G?
- Der Empfänger erhält eine Ciphertext $G = 25$. Sein privater Schlüssel sei $(3, 19)$. Entschlüsseln Sie den erhaltenen Ciphertext.
- Was können Sie über die Eindeutigkeit von T und G bei einem Rabin-Kryptosystem sagen?
- Beurteilen Sie die Sicherheit eines Rabin-Kryptosystems?

Aufgabe 10.5

Ein Systemadministrator hinterlegt das folgende siebenstellige Passwort verschlüsselt in einem Safe:

eDDlIGT

Als Chiffrierfunktion wurde eine umkehrbare, monoalphabetische und affine Tauschchiffre mit einer Blocklänge von einem Zeichen (8 Bit), den Schlüsselparametern $t = 17$ und $k = 5$ sowie dem Modul $n = 67$ gemäß folgender Funktion verwendet.

$$z' = (t \cdot z + k) \bmod n$$

Dabei symbolisiert das Zeichen z ein Klartextzeichen und das Zeichen z' das dazugehörige Chiffretextzeichen.

Die Zeichenkodierung und -dekodierung erfolgte anhand nachstehender Zuordnung:

Zeichen	0	1	...	9	a	b	...	z	A	B	...	Z	§	%	&	?	#
zugeordnete Dezimalzahl	0	1	...	9	10	11	...	35	36	37	...	61	62	63	64	65	66

Die Verschlüsselung erfolgte auf einem 64 Bit Windows-Rechner.

- Entwerfen und implementieren Sie ein C-Programm, welches Ihnen alle die für eine affine Tauschchiffre (Ver- und Entschlüsselung) erforderlichen Berechnungen ermöglicht.
- Unter welcher Voraussetzung ist die gegebene Chiffrierfunktion umkehrbar?

- c) Wie lautet die entsprechende Dechiffrierfunktion und welche Schlüsselparameter weist diese auf?
- d) Dechiffrieren Sie nun das hinterlegte Passwort mit Ihrem Programm unter Verwendung der zuvor ermittelten Dechiffrierfunktion und ihrer Schlüsselparameter. Wie lautet das Passwort demnach im Klartext?

Ciphertextzeichen	e	D	D	l	I	G	T
Ciphertextzahlenwert	14	39	39	21	44	42	55
Klartextzahlenwert							
Klartextzeichen							