Computersystemsicherheit – Übungsblatt Nr. 2

Marc Fischlin, Jacqueline Brendel, Christian Janson
TU Darmstadt, 09 November 2018

Gruppenübung. Die Übungsaufgaben in diesem Bereich sind Gegenstand der Übungen in der Woche vom 12.11.2018 – 16.11.2018.

Aufgabe 1 (Verständnisaufgaben). In dieser Aufgabe prüfen wir unser Verständnis über den Inhalt der Vorlesung.

a) Warum sollte man die Blockchiffe DES nicht mehr benutzen?

b) Welche Schlüssellängen werden bei AES verwendet?

c) Was besagt die funktionale Korrektheit eines Public-key Verschlüsselungsverfahren?

d) Auf welchem schwierigen Problem beruht die Sicherheit des Diffie-Hellman Schlüsselaustauschs?

e) Erinnern Sie sich an das RSA-Verschlüsselungsverfahren und formalisieren Sie wie die Verschlüsselung und Entschlüsselung funktioniert.

f) Was ist Hybride Verschlüsselung?

Aufgabe 2 (Euklidischer Algorithmus). In dieser Aufgabe beschäftigen wir uns mit dem *Euklidischen Algorithmus* und dem *Erweiterten Euklidischen Algorithmus*.

Der Euklidische Algorithmus ist ein bekannter Algorithmus mit welchem sich der *größte gemeinsame Teiler* (ggT) zweier natürlicher Zahlen berechnen lässt. Der Algorithmus basiert auf wiederholter Division mit Rest bis die Sequenz terminiert. Der Euklidische Algorithmus beginnt mit den beiden natürlichen Zahlen a und b für welche der ggT bestimmt werden soll. Formal lässt sich der Algorithmus folgendermaßen beschreiben.

$$\begin{aligned} a &= q_1 b + r_1 \quad \text{mit } 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2 \quad \text{mit } 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \quad \text{mit } 0 \leq r_3 < r_2 \\ &\dots \\ r_{n-2} &= q_n r_{n-1} + r_n \quad \text{mit } 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

Diese Sequenz terminiert, da die Reste immer strikt kleiner werden und der letzte Rest r_n ist der ggT von a und b, also $\mathrm{ggT(a, b)} = \mathrm{r_n}$.

a) Berechnen Sie den ggT für $a = 1337$ und $b = 42$.

Mit einer Erweiterung des obigen Algorithmus lassen sich neben dem ggT für zwei natürliche Zahlen a und b noch zwei ganze Zahlen x und y bestimmen, so dass die Gleichung $c \cdot \mathrm{ggT(a,b)} = \mathrm{x \cdot a + y \cdot b}$ erfüllt ist. Dabei gibt es verschiedene Ansätze dies zu tun. Hier stellen wir kurz die *rekursive* Variante vor.
Erstellen Sie eine Tabelle mit 5 Spalten und die Anzahl der Zeilen hängt vom Euklidischen Algorithmus ab.

a	b	q	x	y

Zuerst berechnet man wie zuvor beschrieben den $\mathrm{ggT(a,b)}$ und trägt die entsprechenden Elemente in die Tabelle:

a	b	q	x	y
a	b	q_1		
b	r_1	q_2		
r_1	r_2	q_3		
$\vdots$	$\vdots$	$\vdots$		
r_{n-2}	r_{n-1}	q_n		

Danach berechnet man rekursiv von unten nach oben die Werte für alle x_i und y_i. Dabei gilt die Vorschrift

$$x_i := y_{i+1} \text{ und } y_i := x_{i+1} - q_i \cdot y_{i+1}$$

für $i \in \{1, \ldots, n\}$ mit $x_{n+1} := 0$ und $y_{n+1} := 1$ und erhält folgende Tabelle:

a	b	q	x	y
a	b	q_1	x_1	y_1
b	r_1	q_2	x_2	y_2
r_1	r_2	q_3	x_3	y_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{n-2}	r_{n-1}	q_n	x_n	y_n

Die Werte für x_1 und y_1 liefern die gesuchten Werte x, y, so dass die Gleichung $x \cdot a + y \cdot b = \mathrm{ggt(a,b)}$ erfüllt ist (also $c = 1$). Soll die Gleichung für ein beliebiges Vielfaches des ggT erfüllt sein, müssen die Werte x_1 und y_1 um den Faktor c erweitert werden.
Der Erweiterte Euklidische Algorithmus wird beispielsweise benötigt um im RSA-Verschlüsselungsverfahren das multiplikative Inverse von e, also d, zu bestimmen.

b) Berechnen Sie mit dem Erweiterten Euklidischen Algorithmus $42 \cdot x + 13 \cdot y = 1$ mit $x, y \in \mathbb{Z}$.

c) Berechnen Sie mit dem Erweiterten Euklidischen Algorithmus $483 \cdot x + 136 \cdot y = 3$ mit $x, y \in \mathbb{Z}$.

Aufgabe 3 (Eulersche φ-Funktion). Die Eulersche φ-Funktion ist eine Funktion welche für jede natürliche Zahl n die Anzahl der zu n teilerfremden natürlichen Zahlen bestimmt, die nicht größer als n sind. Formal bedeutet dies

$$\varphi(n) := |\{a \in \mathbb{N} | 1 \leq a \leq n \text{ und } \mathrm{ggT(a,n)} = 1\}|.$$

Es gelten für die Eulersche φ-Funktion folgende Rechenregeln:

- Für $n > 1$ gilt $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$
- Für p ist Primzahl gilt $\varphi(p) = p - 1$ und $\varphi(p^n) = p^{n-1}(p-1)$ für alle $n \in \mathbb{N}$.
- Für $n = p \cdot q$ mit Primzahlen $p \neq q$ gilt $\varphi(n) = (p-1)(q-1)$
- Für teilerfremde Elemente $m, n \in \mathbb{Z}$ (d.h. ggT(m, n) = 1) gilt $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Berechnen Sie die Eulersche φ-Funktion für die Werte $n = 11, 16, 20, 42, 72, 1337$ mithilfe der obigen Rechenregeln.

Aufgabe 4 (RSA). In der Vorlesung haben Sie das RSA-Verschlüsselungsverfahren kennengelernt.

a) Gegeben sei nur der RSA public key mit $pk = (N, e) = (247, 7)$. Verschlüsseln Sie die Nachricht $m = 16$.

b) Entschlüsseln Sie die Nachricht $c = 2$.
Hinweis: Ermitteln Sie zunächst den geheimen/privaten Schlüssel, d.h. den Exponenten d, welcher das multiplikative Inverse zu e mod $\varphi(N)$ ist. Um diesen Exponenten zu berechnen nutzt man den Zusammenhang zwischen public key und secret key aus: $e \cdot d \equiv 1 \bmod \varphi(N)$.

c) Angenommen $p = 5$ und $q = 3$ werden für die Generierung der folgenden RSA-Schlüssel verwendet:

   - $d = 4, e = 2, N = 15$
   - $d = 4, e = 3, N = 15$
   - $d = 3, e = 3, N = 15$

   Welcher dieser Schlüssel ist gültig? Begründen Sie kurz warum.

Aufgabe 5 (Diffie-Hellman Schlüsselaustausch). In der Vorlesung haben Sie den Schlüsselaustausch nach Diffie und Hellman kennengelernt. Dieser ist dazu gedacht, dass zwei Kommunikationspartner, die miteinander verschlüsselt kommunizieren wollen, durch das Schlüsselaustauschprotokoll am Ende einen gemeinsamen Schlüssel besitzen, der für die folgende Kommunikation verwendet wird.

a) Erinnern Sie sich nochmal wie der Diffie-Hellman Schlüsselaustausch funktioniert. Welche Parameter sind jedem zugänglich? Welche Parameter müssen geheim gehalten werden? Formalisieren Sie, dass beide Kommunikationspartner am Ende den gleichen Schlüssel besitzen.

b) Alice und Bob möchten einen gemeinsamen Schlüssel erstellen. Dazu einigen Sie sich auf die Werte $g = 6$ und $p = 11$. Alice wählt $x = 4$ und Bob $y = 9$. Berechnen Sie die Werte X und Y und den gemeinsamen Schlüssel K.

c) Erklären Sie intuitiv warum ein Angreifer, der die gesamte Kommunikation abhört, nicht an den Schlüssel gelangen kann.

d) Der Assistent von Computersystemsicherheit ist dabei, die Klausur zu entwerfen und möchte einzelne Aufgaben an den Professor schicken. Damit den Studierenden diese Aufgaben nicht in die Hände fallen, möchte er die Kommunikation verschlüsseln. Da der Professor sich aber in einem anderen Gebäude befindet, kann der Schlüsselaustausch nicht persönlich erfolgen, sondern muss digital durchgeführt werden. Aus diesem Grund wendet der Assistent das Diffie-Hellman-Schlüsselaustauschverfahren an. Ein Student hat sich jedoch in das Netzwerk gehackt mit dem Ziel die Nachrichten zwischen dem Professor und Assistenten abzufangen und ggf. zu manipulieren.
Überlegen und formalisieren Sie wie der Student diesen Angriff (nachdem er im Netzwerk ist) ausführt. Wie gelangt der Student in den Besitz des geheimen Schlüssels? Warum kann der Student jetzt Nachrichten manipulieren?

Hausübung. Dieser Bereich ist dazu gedacht das Gelernte weiter zu vertiefen. Dazu werden je nach Themen weitere Übungsaufgaben, ergänzende Beweise oder ähnliche Aufgaben gestellt. Die Aufgaben sind freiwillig, können aber, bei erfolgreicher Bearbeitung, zu Bonuspunkten in der Klausur führen. Die Abgabe dieser Übungen erfolgt über **moodle** und kann in Gruppen mit bis zu vier Studenten (aus Ihrer **eigenen** Übungsgruppe) eingereicht werden. Abgaben werden nur als **.pdf-Dateien** akzeptiert. Denken Sie bitte daran, dass Ihre Lösungen nachvollziehbar und entsprechend ausführlich dargestellt werden sollen.

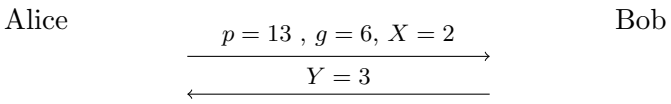
Für Gruppenabgaben ist folgendes zu beachten: Sie müssen in der Abgabe (.pdf-Datei) deutlich und eindeutig kennzeichnen mit welchen Gruppenpartnern die Aufgaben gelöst wurden.

Der Fachbereich Informatik misst der Einhaltung der Grundregeln der wissenschaftlichen Ethik großen Wert bei. Zu diesen gehört auch die strikte Verfolgung von Plagiarismus. Falls dieser Fall eintritt, behalten wir uns das Recht vor für diese Abgabe den jeweiligen Gruppen keine Punkte gutzuschreiben.

Bitte reichen Sie Ihre Abgabe bis **spätestens Freitag 23.11.2018 um 11:40 Uhr** ein. Verspätete Abgaben können **nicht** berücksichtigt werden.

Hausübung 1 (Diffie-Hellman Schlüsselaustausch (2+2 Punkte)). Alice möchte mit Bob auf sichere Weise kommunizieren. In einer Einführungsveranstaltung zur Kryptographie erfährt Alice von dem Diffie-Hellman Schlüsselaustauschverfahren und möchte dieses dafür verwenden.

a) Sie beobachten folgende Konversation zwischen Alice und Bob.



Finden Sie den vereinbarten Schlüssel.

---

b) Alice entscheidet sich um ihren Rechenaufwand zu reduzieren eine additive Gruppe für den Diffie-Hellman-Schlüsselaustausch zu verwenden, d.h. statt $X = g^a$ verwendet sie jetzt $X = g \cdot a$.
Begründen Sie, warum das keine gute Idee ist.

Hausübung 2 (RSA (2 Punkte)). Letztes Semester haben nur die folgenden 3 Studenten an der Klausur zur Vorlesung "Unsichere Kryptosysteme" teilgenommen:

Name	Matrikelnummer
Alice	174458
Bob	217632
Charlie	224710

Die Menge an möglichen erreichbaren Noten war

$$\{1.0, 1.3, 1.7, 2.0, 2.3, 2.7, 3.0, 3.3, 3.7, 4.0, 5.0\}.$$

Nach der Klausur wurden die Noten mittels des RSA-Verfahrens verschlüsselt und ans Studienbüro weitergeleitet. Der benutzte public key ist $pk = (N, e) = (111791377, 3)$. Für jeden Teilnehmer wird die jeweilige Matrikelnummer als $x_1x_2x_3x_4x_5x_6$ interpretiert und mit der erreichten Note $y_1.y_2$ zu dem String $x_1x_2x_3x_4x_5x_6y_1y_2$ codiert. Schließlich wird dieser mit dem obigen public key verschlüsselt und der Ciphertext übermittelt.[1] Folgende Ciphertexts wurden ans Studienbüro geschickt:

$$106894622, \quad 54756549, \quad 49966544$$

In jedem dieser Ciphertexte steht jeweils die Note eines Teilnehmers verschlüsselt und diese Reihenfolge muss nicht mit der obigen Tabelle übereinstimmen.
Obwohl es im Allgemeinen als schwierig gilt die RSA-Verschlüsselung ohne weitere Kentnisse zu invertieren ist es in diesem Fall relativ einfach herauszufinden welche Note Alice in der Klausr erreicht hat. Welche Note hatte sie?

Hausübung 3 (RSA (1+1+2 Punkte)). Alice und Bob haben von dem RSA-Verschlüsselungsverfahren gehört und möchten sich das jetzt gerne etwas genauer ansehen.

a) Gegeben ist ein RSA-Modulus $N = p \cdot q$ mit $N = 77$ und $p = 7, q = 11$ bekannt. Weiterhin ist der public key $pk = (N, e) = (77, 6)$ und Alice möchte mit diesem Schlüssel $m_1 = 5$ und $m_2 = 6$ verschlüsseln. Da Alice aber nicht mehr weiß wie das RSA-Verfahren funktioniert benötigt sie Ihre Hilfe.
Berechnen Sie mit Hilfe des RSA-Verfahrens die Verschlüsselungen von m_1 und m_2.

b) Vergleichen Sie die beiden Ciphertexte aus a). Was fällt Ihnen aus? Warum entsteht dieses Ergebnis?

[0] Wir haben z.B. in Aufgabe 4b) gesehen, dass man mit dem erweiterten Euklidischen Algorithmus leicht multiplikativ inverse Elemente berechnen kann.

[1] Angenommen Bob hätte eine 5.0 in der Klausur erreicht dann würde der String 21763250 zu 95684781 verschlüsselt werden.

c) Bob besitzt den öffentlichen RSA-Schlüssel $(N, e) = (3127, 6)$ mit $N = pq$.
Warum ist dies kein gültiger öffentlicher RSA-Schlüssel? Ändern Sie den ungültigen Anteil von Bobs öffentlichem Schlüssel minimal so ab, dass er gültig wird, und berechnen Sie anschließend den zugehörigen privaten Schlüssel d für ihn.