Vorbemerkungen

Die Abgabe erfolgt online unter folgender Adresse:
https://svs.informatik.uni-hamburg.de/submission/for/gss15-5.

Die Aufgaben auf diesem Übungsblatt dienen zur Vermittlung und Vertiefung von Wissen im Bereich der Kryptographie. Um sich einen Überblick über das Thema zu verschaffen, empfehlen wir die Lektüre der folgenden Online-Quellen:

1. Leibniz-Rechenzentrum: *Verschlüsselung, digitale Signaturen, Zertifikate*, 2005.
   URL: **http://www.lrz.de/services/pki/einf/**
2. Bundesamt für Sicherheit in der Informationstechnik: *M 3.23 Einführung in kryptographische Grundbegriffe*, in: IT-Grundschutz-Kataloge, 2012.
   URL: **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03023.html**

Unterstützende Informationen zur Lösung der Aufgaben können Sie dem folgenden Buch entnehmen: Spitz et al.: *Kryptographie und IT-Sicherheit – Anwendungen und Grundlagen*, Vieweg+Teubner, Wiesbaden, 2011. Vom Campus-Netzwerk aus haben Sie Zugriff auf den **Volltext**. (URL: **http://dx.doi.org/10.1007/978-3-8348-8120-5**). Insbesondere die Kapitel 1 (Ziele und Wege der Kryptographie), 4 (Asymmetrische Chiffren) sowie 5 (Authentifikations-Protokolle) sind für die Aufgaben relevant.

Aufgabe 1: Zentrale Begriffe der Kryptographie

1. **Unterschiedliche Chiffren (Pflicht; 2 Punkte)** – Was ist der Unterschied zwischen einem symmetrischen und einem asymmetrischen Kryptosystem?
2. **Hybride Kryptosysteme (Pflicht; 3 Punkte)** – Alice (A) und Bob (B) haben jeweils ein Schlüsselpaar erzeugt, um vertraulich miteinander kommunizieren zu können. Sie verfügen nun jeweils über einen öffentlichen (public) Schlüssel (K_p^A bzw. K_p^B) sowie einen privaten (secret) Schlüssel (K_s^A bzw. K_s^B). Ihre öffentlichen Schlüssel haben die beiden bereits bei einem persönlichen Treffen ausgetauscht. Alice möchte Bob nun eine vertrauliche Nachricht übermitteln.
   a) Unter welchen Umständen wird Alice dazu auf ein sog. *hybrides Kryptosystem* zurückgreifen?
   b) Wie geht Alice im Detail vor, wenn sie ein hybrides Kryptosystem einsetzt?
   c) Wie sieht die übertragene Nachricht in diesem Fall aus?

Aufgabe 2: Parkhaus

In dem kostenpflichtigen Parkhaus eines Einkaufszentrums einer bayrischen Großstadt kommt das neue *iPark secure* zum Erheben der Parkgebühren zum Einsatz. Dieses System gibt beim Einfahren in das Parkhaus an einer Schranke Parktickets auf Karton aus. Auf die Tickets werden Barcodes aufgebracht. Vor dem Verlassen des Parkhauses muss an einem Kassenautomat die Parkgebühr entrichtet werden. Die genaue Höhe wird mit Hilfe der ausgegebenen Karte ermittelt. Die Schranke bei der Ausfahrt öffnet nur, wenn zwischen dem Bezahlvorgang weniger als 10 Minutenn verstrichen sind.

Neben einer Vielzahl von Läden gibt es in dem Einkaufszentrum jedoch zwei Unternehmen, welche ihren Kunden besondere Park-Konditionen einräumen möchten: Ein Einzelhändler bietet an, ab einem Einkaufswert von 15 EUR das Parkticket mit einer Markierung zu versehen (dazu später mehr), die den Kunden 90 Minuten kostenfreies Parken ermöglicht. Ein angeschlossenes Kino erlaubt es hingegen seinen Besuchern (ebenfalls durch Markierung des Parktickets), ihre Fahrzeuge für pauschal 2,50 EUR den ganzen Tag im Parkhaus unterzustellen.

Sie haben sich acht bereits verwendete Parktickets besorgt (siehe Abb. 1). Sie wissen, dass der letzte und vorletzte Barcode (also die beiden rechten Barcodes) bereits durch die Schranke an der Einfahrt auf das Ticket aufgedruckt werden. Der dritte Code von rechts wird nach dem Bezahlvorgang durch den Kassenautomat hinzugefügt – ebenso wie die menschenlesbaren Informationen in der Ecke links unten. Hat man das Kino oder das Geschäft mit den vergünstigten Parkkonditionen besucht, so wird dort noch jeweils ganz links ein Barcode aufgebracht (dieser ist nicht auf allen Tickets vorhanden).

1. **Funktionsweise (Optional)** – Untersuchen und vergleichen Sie die Parktickets und versuchen Sie zu verstehen, wie das System arbeitet. Wie funktioniert es, welche Daten werden vermutlich wie übermittelt und warum wurde es auf diese Art ausgestaltet?
2. **Sicherheitsanalyse (Pflicht; 4 Punkte)** – Weist das System Schwächen auf? Welches Angreifermodell liegt dem System demnach offenbar zu Grunde?
3. **Umsetzung mit kryptographischen Techniken (Pflicht; 4 Punkte)** – Nehmen Sie nun an, dass es nicht möglich ist, Daten zwischen den Komponenten des Systems auf einem anderen Weg als auf dem Ticket zu übermitteln. Wie würden Sie das System durch Einsatz von kryptographischen Techniken gestalten, um Betrug in diesem Fall effektiv zu verhindern? Beschreiben Sie Ihr Parksystem im Detail, auch gerne unter Zuhilfenahme einer Abbildung, und begründen Sie Ihre Entscheidungen.

Aufgabe 3: Authentifizierungsprotokolle

1. **Verschlüsselte Passwort-Übermittlung (Optional)** – Der Nutzer eines Laptops soll sich gegenüber einem Server mit einem Benutzernamen u und einem Passwort p authentisieren. Um zu verhindern, dass Benutzername und Passwort im Klartext übertragen werden, werden diese Daten mit einem in der Vergangenheit einmalig festgelegten Schlüssel k unter Verwendung der Verschlüsselungsfunktion $c = E_k(u, p)$ verschlüsselt. Es wird lediglich c an den Server

Abbildung 1: Park-Tickets des iPark secure Systems (vgl. Aufgabe 2)

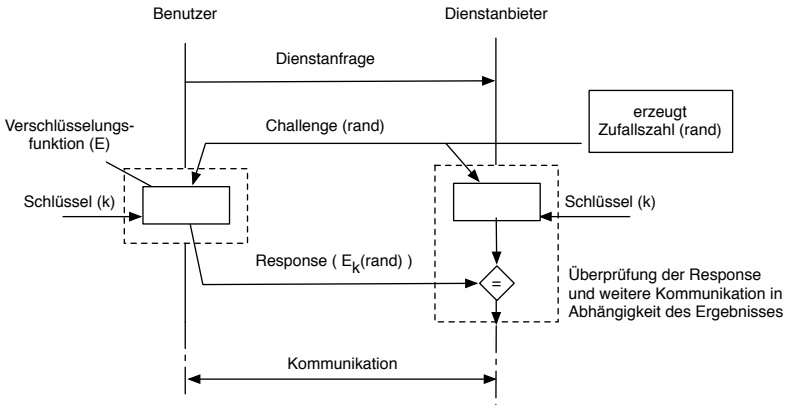

Abbildung 2: Einseitige Challenge-Response-Authentifizierung (vgl. Aufgabe 3)

übermittelt. Welche Schwäche weist dieses Protokoll gegenüber einem passiven bzw. aktiven Angreifer auf der Kommunikationsstrecke auf?

2. **Authentifikationssystem auf Basis indeterministischer symmetrischer Verschlüsselung (Pflicht; 2 Punkte)** – Ein befreundeter Systemadministrator macht den Vorschlag, das oben genannte Verfahren wie folgt zu verbessern: Der Nutzer soll nun $c = E_k(r, u, p)$ übertragen, wobei r eine selbst gewählte, große (kryptographisch sicher erzeugte) Zufallszahl ist, die den anderen Daten vor der Verschlüsselung vorangestellt wird. Wie beurteilen Sie die Sicherheit dieser Realisierung, d.h. welche Angriffe werden dadurch verhindert, welche sind weiterhin möglich?

3. **Challenge-Response-Authentifizierung (Pflicht; 2 Punkte)** – Abbildung 2 zeigt ein einseitiges Challenge-Response-Authentifizierungsverfahren auf Basis eines symmetrischen Kryptosystems. Welche Angriffe, die bei Teilaufgabe b) noch möglich waren, werden dadurch verhindert, welche sind weiterhin erfolgreich?

4. **Sichere Challenge-Response-Authentifizierung (Optional)** – Das Protokoll aus der vorherigen Teilaufgabe weist eine Schwachstelle auf: Ein Angreifer kann sich gegenüber dem Benutzer als Dienstanbieter ausgeben, ohne dass der Benutzer dies erkennen kann. Erweitern Sie das Challenge-Response-Protokoll dahingehend, dass sich auch der Benutzer sicher sein kann, mit dem richtigen Dienstanbieter verbunden zu sein. Erstellen Sie dazu eine aussagekräftige Abbildung bzw. führen Sie genau auf, welche Nachrichten Nutzer und Server gegenseitig übermitteln und erläutern Sie, warum der Angriff nun nicht mehr funktioniert. Verwenden Sie dabei weiterhin ein symmetrisches Kryptosystem.

Aufgabe 4: „Mensch ärgere Dich nicht“ über das Telefon

Alice und Bob spielen leidenschaftlich gern das Brettspiel „Mensch ärgere dich nicht“. Alice macht gerade Urlaub in Alicante (Spanien), während Bob zu Hause in Bobingen geblieben ist. Davon

wollen sich die beiden jedoch nicht am Spielen hindern lassen. Außer einem altmodischen Mobiltelefon (ohne Internetzugang), dem „Mensch ärgere dich nicht“-Brettspiel und einem Laptop (auch ohne Internetzugang) hat Alice nichts dabei. Bob besitzt ebenfalls ein Telefon, ein Brettspiel und einen Laptop.

1. **Protokoll (Optional)** – Überlegen Sie sich ein möglichst einfaches Protokoll, mit dem die beiden eine Partie über das Telefonnetz spielen können. Welche weiteren Voraussetzungen bzw. Vereinbarungen sind hierfür nötig? Welche Spielzüge müssen im Protokoll abgebildet werden können?
2. **Würfeln über Telefon (Optional**) – Ihr Vorschlag aus Teilaufgabe 1 stößt auf wenig Akzeptanz. Alice und Bob mögen sich zwar gerne, aber bei „Mensch ärgere Dich nicht“ verstehen Sie keinen Spaß: Sie befürchten, dass beim Würfeln betrogen wird. Schlagen Sie ein Protokoll vor, bei dem keiner hinsichtlich des Würfelergebnisses schummeln kann.

Aufgabe 5: RSA-Verfahren

Das Verfahren von Rivest, Shamir und Adleman (kurz: RSA) ist eines der am weitesten verbreiteten asymmetrischen Kryptographieverfahren. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nur mit extrem hohen Aufwand aus dem öffentlichen Schlüssel berechnet werden.

1. **Grundlagen (Optional)** Wie wird beim RSA-Verfahren das Schlüsselpaar erzeugt? Wie erfolgen Verschlüsselung und Entschlüsselung? Worauf basiert die unterstellte Sicherheit des RSA-Verfahrens? Was ist die häufigste Anwendungform von RSA in der Praxis?
2. **Anwendung (Pflicht; 6 Punkte)** Gegeben ist der in Abbildung 3 dargestellte Schlüsseltext. Dieser wurde durch Anwendung des RSA-Verfahrens erzeugt. Dabei wurde der ASCII-Code jedes einzelnen Zeichens separat verschlüsselt. Das dabei verwendete Schlüsselpaar wurde aus folgenden (zu Anschauungszwecken verwendeten, völlig unsicheren) Basiswerten erzeugt: $p = 281$, $q = 389$, $e = 67$

   Ihre Aufgabe: Ermitteln Sie den zugehörigen Entschlüsselungsexponenten d und dekodieren Sie damit den gegebenen Schlüsseltext Zeichen für Zeichen. Wie lauten d und der ursprüngliche Klartext? Bitte fügen Sie Ihrer Lösung auch Ihren Quelltext hinzu, falls Sie die Aufgabe programmatisch lösen.

   Hinweis: Viele Skriptsprachen (wie Ruby) können mit den bei der Lösung u. U. entstehenden großen Integerzahlen umgehen. Falls Sie diese Aufgabe mit Java bearbeiten wollen, sollten Sie die Klasse *BigInteger* verwenden und sich die Methode *modPow* näher ansehen.
3. **Sichere Implementierung (Optional)** Das von Ihnen in der vorherigen Teilaufgabe verwendete (deterministische) RSA-Verfahren ist gegen eine Chosen-Plaintext-Attack anfällig. Erläutern Sie dies an einem Beispiel und stellen Sie dar, wie der Angriff durch eine kleine Erweiterung verhindert werden kann (p, q und e sollen unverändert bleiben).

103625, 71396, 5872, 102989, 10232, 36843, 71765, 5872, 10232, 14809, 108822, 108822, 69296, 32156, 36704, 105697, 71396, 25948, 71396, 102989, 10232, 25948, 71765, 64024, 36843, 10232, 16718, 105867, 36704, 34992, 5872, 64024, 36843, 5872, 10232, 2762, 73111, 5872, 19729, 5872, 64024, 10232, 109169, 71765, 1086, 73111, 57424, 71765, 34992, 60372, 10232, 108822, 1086, 73111, 71396, 57424, 40412, 40412, 71765, 5872, 36704, 5872, 82037, 10232, 86175, 64024, 34992, 102989, 5872, 71765, 16718, 5872, 102989, 19729, 105867, 36843, 5872, 36704, 36704, 5872, 82037, 10232, 61644, 105697, 71765, 64024, 36265, 105867, 109169, 10232, 2762, 105697, 36265, 36704, 5872, 25948, 82037, 10232, 36843, 71765, 5872, 10232, 89982, 27255, 64024, 69296, 62098, 108822, 71765, 1086, 73111, 5872, 102989, 73111, 5872, 71765, 57424, 10232, 61865, 105867, 64024, 10232, 35203, 105697, 25948, 25948, 109169, 105867, 5872, 102989, 57424, 5872, 102989, 64024, 10232, 71396, 64024, 36843, 10232, 36843, 105697, 40412, 71396, 34992, 5872, 73111, 105867, 5872, 102989, 71765, 34992, 5872, 10232, 86175, 64024, 34992, 102989, 71765, 16718, 16718, 5872, 82037, 10232, 57837, 71396, 34992, 105697, 64024, 34992, 25948, 69296, 10232, 71396, 64024, 36843, 10232, 57837, 71396, 34992, 102989, 71765, 16718, 16718, 25948, 78325, 105867, 64024, 57424, 102989, 105867, 36704, 36704, 5872, 82037, 10232, 102020, 71765, 105867, 19729, 5872, 57424, 102989, 71765, 25948, 1086, 73111, 5872, 10232, 52356, 5872, 102989, 16718, 105697, 73111, 102989, 5872, 64024, 82037, 10232, 2762, 71765, 19729, 71765, 64024, 34992, 69296, 86175, 57424, 57424, 105697, 1086, 78325, 10232, 71396, 64024, 36843, 10232, 35203, 105867, 109169, 5872, 102989, 69296, 86175, 64024, 105697, 36704, 40103, 25948, 71765, 25948, 82037, 10232, 14809, 102989, 71396, 64024, 36843, 36704, 105697, 34992, 5872, 64024, 10232, 36843, 5872, 102989, 10232, 32156, 102989, 40103, 108306, 57424, 105867, 34992, 102989, 105697, 108306, 73111, 71765, 5872, 820 37, 10232, 86175, 71396, 57424, 73111, 5872, 64024, 57424, 71765, 16718, 71765, 78325, 105697, 57424, 71765, 105867, 64024, 25948, 108306, 102989, 105867, 57424, 105867, 78325, 105867, 36704, 36704, 5872, 82037, 10232, 36843, 105697, 25948, 10232, 61644, 108822, 86175, 69296, 52356, 5872, 102989, 16718, 105697, 73111, 102989, 5872, 64024, 10232, 71396, 64024, 36843, 10232, 64024, 105697, 57424, 71396, 5872, 102989, 36704, 71765, 1086, 73111, 10232, 105697, 36704, 36704, 5872, 10232, 105697, 64024, 36843, 5872, 102989, 5872, 64024, 10232, 59390, 64024, 73111, 105697, 36704, 57424, 5872, 82037, 10232, 36843, 71765, 5872, 10232, 109169, 71765, 102989, 10232, 71765, 64024, 10232, 36843, 5872, 102989, 10232, 27255, 5872, 36265, 71396, 64024, 34992, 10232, 71396, 64024, 36843, 10232, 36843, 5872, 102989, 10232, 52356, 105867, 102989, 36704, 5872, 25948, 71396, 64024, 34992, 10232, 36265, 5872, 73111, 105697, 64024, 36843, 5872, 36704, 57424, 10232, 73111, 105697, 36265, 5872, 64024, 10232, 60372, 69296, 62098

Abbildung 3: Schlüsseltext für Aufgabe 5.2