Institut für Theoretische Informatik
Jun.-Prof. Dr. D. Hofheinz

Stammvorlesung Sicherheit im Sommersemester 2014

Übungsblatt 4

Hinweis: Übungsblätter können freiwillig bei Florian Böhl, Raum 255, Geb. 50.34 („Info-Bau“) bis zur Übung am 12.6.14 zur Korrektur abgegeben werden. Die Korrektur dient nur der Selbstkontrolle; es gibt keine Punkte und keinen Klausur-Bonus.

Aufgabe 1. Wir instanziieren das ElGamal-Verschlüsselungsverfahrens aus der Vorlesung über der Gruppe $\mathbb{G} := \mathbb{Z}_{59}^*$ und wählen $g := 27$ (g erzeugt nicht $\mathbb{G}$ sondern die Untergruppe der Quadrate[1] von $\mathbb{Z}_{59}^*$ der Ordnung 29). Der Einfachheit halber sei der geheime Schlüssel sk in dieser Aufgabe direkt der geheime Exponent und der öffentliche Schlüssel $pk = g^{sk}$. (In der Vorlesung enthielten die Schlüssel jeweils noch die Gruppe $\mathbb{G}$ und g.)

(a) Berechnen Sie zu dem geheimen Schlüssel $sk := 20$ den öffentlichen Schlüssel pk.

(b) Berechnen Sie das Chiffrat c zu der Nachricht $m := 22$ unter dem in (a) berechneten Schlüssel pk, wobei Sie $r := 12$ als Zufall verwenden.

(c) Es sei $c := (51, 8)$ ein Chiffrat. Verwenden Sie den geheimen Schlüssel aus (a), um die als Gruppenelement codierte Nachricht $m \in \mathbb{G}$ zu berechnen.

Hinweis: Versuchen Sie, sich die Rechenregeln der Modulo-Arithmetik und für endliche Gruppen zunutze zu machen. Sie sollten dann in der Lage sein, diese Aufgabe größtenteils „im Kopf“ zu lösen.

Aufgabe 2. Wir beschäftigen uns mit der Homomorphie des ElGamal-Verschlüsselungsverfahrens. Sei $\mathbb{G}$ eine öffentlich bekannte Gruppe primer Ordnung p mit Generator g. Weiterhin seien zwei Parteien A und B gegeben. A kennt ein Polynom

$$f(x) := \sum_{i=0}^{d} a_i x^i \in \mathbb{F}_p[X]$$

($\mathbb{F}_p$ ist hier der Körper mit p Elementen). B möchte für einige Elemente $E \subseteq \mathbb{F}_p$ testen, ob sie Nullstellen von f sind. A will f allerdings nicht einfach preisgeben (ist aber bereit B den Grad d von f mitzuteilen). Entwerfen Sie ein kryptographisches Protokoll auf Basis des ElGamal-Verschlüsselungsverfahrens, dass die gewünschte Funktionalität realisiert. Gehen Sie dabei davon aus, dass A, B beide kooperativ agieren (d.h. sie halten sich an das vorgegebene Protokoll), dabei aber versuchen, so viel wie möglich zu erfahren[2]. Sie dürfen außerdem annehmen, dass A und B bereits über einen sicheren Kanal kommunizieren; an dieser Stelle kommt also kein Angreifer ins Spiel. Was erfährt A bei Ihrem Protokoll günstigstenfalls über die Menge E? Was B günstigstenfalls über f? Könnte eine bessere Lösung existieren?

[1] Die Untergruppe der Quadrate von $\mathbb{Z}_{59}^*$ besteht aus den Elementen $\{x^2 \bmod 59 : x \in \mathbb{Z}_{59}^*\}$

[2] Dieses „honest but curious“-Verhalten ist in der IT-Sicherheit oft ein realistisches Szenario.

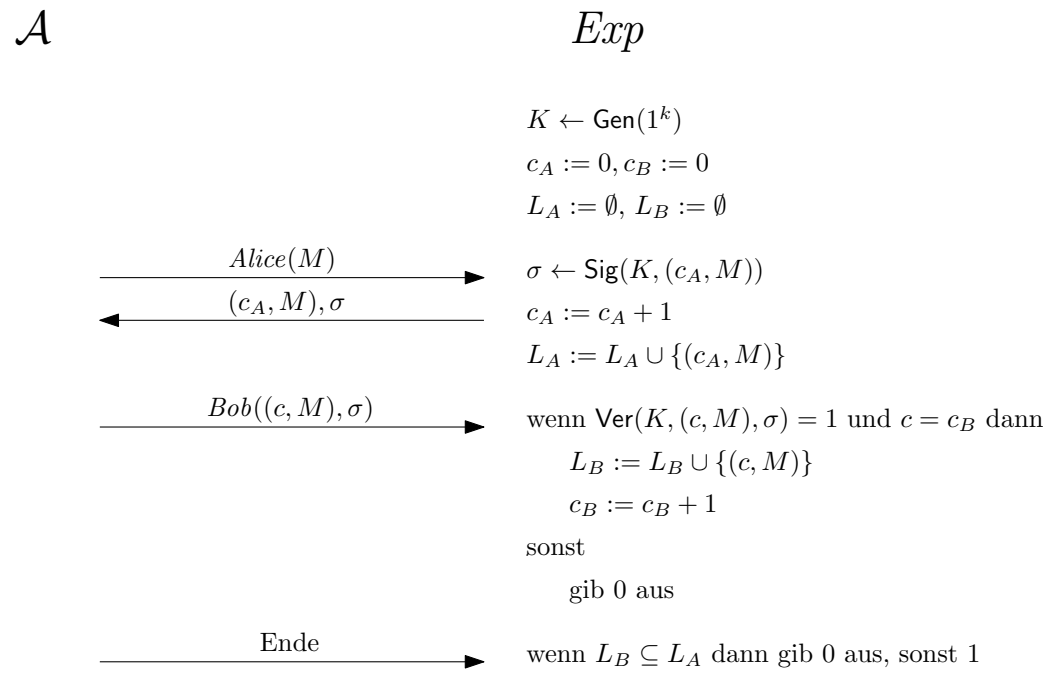

Abbildung 1: Sicherheitsexperiment für einen authentifizierten Kanal.

Aufgabe 3. Es sei $\mathsf{MAC} = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ ein MAC-Verfahren. Wir wollen MAC benutzen, um einen authentifizierten Kanal zwischen zwei Parteien $A(lice)$ und $B(ob)$ zu realisieren. (Genau genommen betrachten wir der Einfachheit halber nur Nachrichten, die von A an B geschickt werden). Wir gehen davon aus, dass A und B bereits einen gemeinsamen Schlüssel K ausgetauscht haben. Die Sicherheit des Kanals beschreiben wir mit dem Spiel in Abbildung 1: Das Experiment generiert zunächst einen Schlüssel K und initialisiert Zähler für die Parteien A und B sowie Listen der akzeptierten Nachrichten L_A und L_B. Der Angreifer kann nun beliebig oft eine der folgenden Anfragen stellen:

- $Alice(M)$: Der Angreifer kann Alice eine Nachricht M schicken lassen. Alice signiert das Paar aus Nachricht und ihrem aktuellen Zähler. Das Zähler/Nachrichten-Paar wird der Liste L_A der von Alice geschickten Nachrichten hinzugefügt.
- $Bob((c, M), \sigma)$. Der Angreifer kann Bob ein Zähler/Nachrichten-Paar (c, M) und eine Signatur σ empfangen lassen. Bob prüft Signatur und Zählerstand. Ist beides valide, fügt er das Zähler/Nachrichten-Paar der Liste seiner empfangenen Nachrichten hinzu. Ansonsten bricht das Experiment mit 0 ab (der Angreifer verliert).
- *Ende*: Der Angreifer beendet das Experiment. Sind die Nachrichten, die Bob akzeptiert hat, eine Untermenge der Nachrichten, die Alice geschickt hat, so verliert der Angreifer (0-Ausgabe). Ansonsten gewinnt er (1-Ausgabe).

Beweisen Sie, dass kein Angreifer das beschriebene Spiel für ein EUF-CMA-sicheres Signaturverfahren MAC mit nicht-vernachlässigbarer Wahrscheinlichkeit gewinnen kann. Geben Sie hierzu an, wie Sie einen Angreifer $\mathcal{A}$ für das Spiel in Abbildung 1 benutzen können, um einen Angreifer $\mathcal{B}$ für das EUF-CMA-Spiel zu konstruieren. Hierbei sollte $\mathcal{B}$ nicht-vernachlässigbaren Erfolg haben, sofern $\mathcal{A}$ nicht-vernachlässigbaren Erfolg hat.

Diese Konstruktion eines authentifizierten Kanals aus einem MAC unter Zuhilfenahme von Zählern ist in der Praxis üblich und wird (sehr ähnlich) beispielsweise in Transport-Layer-Security-Verschlüsselungsprotokoll (TLS-Protokoll) verwendet. Überlegen Sie sich, warum ein Zähler eingeführt und mit der Nachricht authentifiziert wird.

Aufgabe 4. Der ebenso geniale wie durchtriebene Wissenschaftler und Superbösewicht Doktor Meta ist beunruhigt. Erneut schweift sein Blick über eine Anordnung von Monitoren, die die Videos der über seine geheime Liegenschaft verteilten Überwachungskameras direkt im Kontrollraum anzeigen. Er lehnt sich zurück. Sieben Tage ist es nun her, dass er Annette Gui, die Geliebte seines Gegenspielers Max Security, in seine Gewalt bringen konnte. Seitdem hat er sein Anwesen keine wache Sekunde aus dem Auge gelassen. Wird er Anettes Aufenthaltsort noch lange genug vor Max Security geheim halten können, um seinen gewieften Plan realisieren zu können? Eigentlich kann sie niemand hier erwarten. Doktor Meta seufzt und blickt auf den Kalender. Schon am kommenden Montag beginnt SuperCon – das ultimative Jahrestreffen der Superbösewichte, das er sich auf keinen Fall entgehen lassen will. Die Überwachung des Anwesens muss er in dieser Zeit seinen Schergen überlassen. Sorgenvoll wendet er sich seiner Tastatur zu und beginnt zu tippen.

Max Security reibt sich die Augen. Sein normalerweise ruhiger tiefer Schlaf ist seicht und von Alpträumen durchzogen seit Anette verschwunden ist. Obwohl ihre Beziehung wahrlich nicht als sorgenfrei beschrieben werden kann, wünscht er sich nichts sehnlicher als Anette wieder an seiner Seite zu haben. Ohne sie fühlt er sich nicht komplett. Max' Bewusstsein nimmt erst jetzt das Piepen und die grüne Kontrollleuchte seiner Superbösewichtüberwachungsanlage wahr. Noch schlaftrunken dreht er sich aus dem Bett und wendet sich einem Monitor zu. Zahlenkolonnen rasen über das Display – eine abgefangene Nachricht von Doktor Meta. Sofort ist Max hellwach. Wird er endlich einen Hinweis auf Anettes Aufenthaltsort finden?

Doktor Meta verwendet das ElGamal-Verschlüsselungsverfahren. Auf der Vorlesungswebseite finden Sie zwei Dateien

- `Sicherheit_UE04_A4_Oeffentlich.txt` enthält einen primen Modulus p, einen Generator g für die multiplikative Gruppe $\mathbb{Z}_p^*$ ($\langle g \rangle = \mathbb{Z}_p^*$) und den verwendeten öffentlichen Schlüssel pk.
- `Sicherheit_UE04_A4_Chiffrat.txt` enthält die abgefangene Nachricht. Aus technischen Gründen muss Doktor Meta seine Nachricht zeichenweise in ASCII-Codierung (d.h. `A` $\mapsto$ 65) verschlüsseln und verwendet nur Großbuchstaben (keine Umlaute, kein scharfes S).