Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 18.12.2015
Abgabe: Mo. 04.01.2016 bis 14:45 Uhr

Einführung in Kryptographie

WS 2015/2016

⋆ Weihnachtsübungszettel ⋆

– Ausschließlich elektronische Abgabe per koaLA –

AUFGABE 1 (10 Punkte)**:**
Stellen Sie sich vor, Sie möchten als Geheimdienstmitarbeiter der *AG-A Agency* den feindlichen Geheimdienst *AG-B Agency* ausspionieren.
Über die Feiertage hinweg hat sich *AG-B Agency* dafür entschieden, ihren Agenten neue Aufträge über die `https://groups.upb.de/fg-bloemer/` Webseite zuzustellen. Über einen Inside Job haben wir herausgefunden, dass die Agenten-IDs identisch zu unseren IMT Logins sind. – Wir fragen uns nun, ob wir Doppelagenten beschäftigen. –
Ihr Auftrag lautet:

a) Stellen Sie das Passwort zu Ihrer ID (IMT Login) sicher.

   - Wenn Sie in einer Gruppe arbeiten, nutzen Sie ausschließlich einen der IMT Logins Ihrer Gruppe.

b) Wie lautet der geheime Auftrag im System der *AG-B Agency* zu Ihrer ID?

Die Abgabe besteht aus:

- Dem benutzten IMT Login und der Auftragsnummer, die im System der *AG-B Agency* nach dem erfolgreichen Login angezeigt wird.
- Einer kurzen Beschreibung des Lösungswegs.

Tipps:

- Unser Informant hat uns mitgeteilt, dass jede ID ein festes Passwort hat, das man sich verschlüsselt über den *Passwort vergessen* Link anzeigen lassen kann.
- Nach ersten Analysen teilte uns unser Informant mit, dass aufgrund der Größe des RSA Modul ein Computerprogramm nötig sein wird, um das Passwort zu ermitteln.
- Abschließend weist unser Informant darauf hin, dass es mit Java-Kenntnissen vorteilhaft wäre, sich die *BigInteger* Klasse genauer anzuschauen, um die nötigen Berechnungen durchzuführen.
- – Denken Sie an die Angriffe im RSA Abschnitt aus der Vorlesung –

AUFGABE 2 (10 Punkte)**:**
Sei im Folgenden $n \coloneqq 1024$. Eine Permutation auf der Menge $\{1, \ldots, n\}$ ist eine bijektive Abbildung $\{1, \ldots, n\} \to \{1, \ldots, n\}$. Gegeben sei eine Permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$, definiert durch die Datei `Weihnachtszettel_permutation.txt`[1]: In der i-ten Zeile der Datei steht das Bild von i unter π, z.B. $\pi(2) = 190$.
Die Menge der Permutationen auf $\{1, \ldots, n\}$ bildet eine Gruppe zusammen mit der Verknüpfung $\circ$. Diese ist wie folgt definiert: Für zwei Permutationen π_1, π_2 ist $\pi_1 \circ \pi_2 := \pi_3$ mit $\pi_3(x) = \pi_1(\pi_2(x))$ für $x \in \{1, \ldots, n\}$.

a) Sei $e = 10^{18}$. Berechnen Sie $\pi' \coloneqq \pi^e$.

b) Gegeben sei $(\pi'(m_1), \ldots, \pi'(m_7)) \coloneqq (336, 139, 499, 772, 139, 135, 69)$.
Berechnen Sie $m_1, \ldots, m_7$.

c) Betrachten Sie das Codewort $m_1, \ldots, m_7$ als Folge von Unicode Codepunkten. Nutzen Sie eine Unicode-Tabelle (z.B. `http://www.utf8-chartable.de/unicode-utf8-table.pl?utf8=dec`), um das durch $m_1, \ldots, m_7$ kodierte Wort zu erhalten.

Die Abgabe sollte $(m_1, \ldots, m_7)$, das Codewort und eine Beschreibung des Lösungswegs inklusive verwendetem Code, zur Berechnung, enthalten. Der Code ist elektronisch über koaLA abzugeben.
Tipp:

- Es gibt einen Algorithmus im RSA-Foliensatz, der für effiziente Berechnung von m^e in RSA verwendet wurde, aber unverändert für allgemeine Gruppen funktioniert.

[1]Die Datei kann heruntergeladen werden unter `https://www-old.cs.uni-paderborn.de/fileadmin/Informatik/AG-Bloemer/lehre/2015/ws/efk/Weihnachtszettel_permutation.txt`