Fachhochschule Nordwestschweiz
Hochschule für Technik

Applikationssicherheit

4. November 2013

Laborübung 1

Inhaltsverzeichnis

Thomas Baumann & Egemen Kaba

1 Ressourcen

Die Dateien wurden in ISO-8859-1 kodiert, damit die Umlaute korrekt dargestellt und ausgelesen werden können.

original.txt
Die originale Textnachricht von Bob als Plaintext.

Patterns.txt
Patterns, die benutzt werden, um eine gefälschte Nachricht zu generieren, welche den gleichen Hashwert, wie die Originalnachricht hat.
Die Form dazu ist folgende:

- Je Pattern existiert eine Linie in der Datei
  - Gesamthaft also 32 Linien $\Longrightarrow$ Bits in einem Integer
- Je Linie existieren zwei Möglichkeiten, die durch eine vertikale Trennlinie unterteilt sind (Text 1 |Text 2) $\Longrightarrow$ 0 bzw. 1 eines Bits

Patterns_Org.txt
Patterns, um eine Originalnachricht zu erstellen.
Sie ist gleich aufgebaut, wie *Patterns.txt*.

2 Klassen

Implementierungsdetails siehe Sourcecode.

Start
Dies ist ein möglicher Startpunkt der Applikation. Dabei wird die vorgegebene originale Nachricht verwendet und permutierende Fälschungen erstellt.

StartPermutation (main)
Dies ist der zweite mögliche Startpunkt der Applikation. In diesem Fall werden sowohl permutierende Fälschungen, als auch permutierende originale Nachrichten erstellt. Dabei werden zwei verschiedene Texte pro Aufruf erstellt.

TextGenerator
Diese Klasse liest ein Pattern-Datei ein und generiert daraus bei Aufruf der entsprechenden Methode Texte. Da ein Pattern-Datei genau 32 Möglichkeiten hat ein Text zu generieren, wird auf Basis eines Integers gearbeitet, um zu bestimmen, welche Möglichkeit (0 oder 1 =¿ links oder rechts) auszuwählen ist. Dieser Integer kann entweder inkrementell oder randomisiert gewählt werden.

DESHash
In dieser Klasse ist die DES-Funktion aus der Aufgabenstellung implementiert. Dabei werden

die Klassen DESEngine für den DES und PaddedBufferedBlockCipher, um die Engine in einer BlockCipher auszuführen, von Bouncy Castle verwendet.

Es wurde die Methodik der Aufgabenstellung übernommen. Einzige Anmerkung gilt es bei dem Ergebnis des DES zu machen. Und zwar arbeitet DES mit zwei 64 Bit Blöcken. Bei der Weiterverwendung des Outputs als ein 64 Bit Block müssen diese zwei Blöcke dementsprechend mit xor vereint werden.

3 Ergebnisse

Es wurden zwei Varianten bzw. Interpretationsmöglichkeiten der Aufgabestellung implementiert.

Variante 1
Die erste Variante sieht vor, dass ein festes originales File vorhanden ist. Die Fälschungen werden anhand eines Pattern-Files generiert.
Als Startmethode wird hier die Klasse Start genommen. Diese Variante erzielte jedoch kein Ergebnis, auch wenn sie über Nacht, also mehrere Stunden, lief.

Variante 2
Die zweite Variante sieht vor, dass Originale, sowie Fälschungen anhand je eines Pattern-Files generiert werden.
Als Startmethode wird hier die Klasse StartPermutation genommen und die gewünschte Anzahl Kollisionen, nach der gesuchten werden soll, kann in der Variable count angegeben werden.
Die Laufzeit beträgt ca. 5 Minuten für fünf Kollisionen. Dies kann jedoch variieren, da mit der randomisierten Textgenerierung früher oder später ein entsprechender Text erstellt wird.

Diese Variante erzielte folgendes Ergebnis mit 5 Kollisionen:

Found Hash: 574314342
Strings mapping to that Hash:
1) Meine liebe Alice, ich bedanke mich vom Herzen für Deinen sehr willkommenen Auftrag. Ich möchte Dich vertraulich aufmerksam machen, dass unsere Ingenieure etwas Sensationelles in den Kächern halten : SunShineForever. Du kannst Dir plastisch denken was dahinten steckt! Du wirst die einzige sein, eine ansehnliche Menge Muster kostenlos zu erhalten. Ich bitte Dich den Betrag von 100.000.- Schweizer Franken auf das Konto mit der Nr. 222-1101.461.12 der Bank ABC AG, in Basel CH zu überweisen.Ich freue mich Dir geholfen zu haben und verbleibe ich freundlichen Grüssen. Dein Bob, CEO
2) liebe Alice, ich bedanke mich aufrichtig für den erfreulichen Lieferungsvertrag. Ich möchte Dich aufmerksam machen, dass unsere Ingenieure etwas Sensationelles in den Reagenzgläsern halten : SunShineForever. Du kannst Dir plastisch vorstellen was dahinten steckt! Du wirst die erste sein, eine ansehnliche Anzahl Fläschen gratis zu erhalten. Ich bitte Dich die Sum-

me von 100.000.- CHF auf das Konto mit der Nr. 222-1101.461.10 von der Bank ABC AG, in Basel zu überweisen.Ich freue mich Dir gedient zu haben und schliesse ich freundlichen Grüssen. Bob, CEO

Found Hash: -2128439365
Strings mapping to that Hash:
1) liebe Alice, ich bedanke mich vom Herzen für den sehr willkommenen Auftrag. Ich möchte Deine Firma vertraulich aufmerksam machen, dass wir etwas Herausragendes in den Reagenzgläsern halten : SunShineForever. Du kannst Dir vorstellen was dahinten steckt! Du wirst die erste sein, eine ansehnliche Anzahl Muster gratis zu kriegen. Ich bitte Dich die Summe von 100.000.- Schweizer Franken auf das Konto mit der Nr. 222-1101.461.12 der Bank ABC AG, 4001 Basel zu überweisen.Ich freue mich Dir geholfen zu haben und verbleibe ich mit lieben Grüssen. Dein Bob, Geschäftsführer
2) Meine liebe Alice, ich bedanke mich aufrichtig für den erfreulichen Lieferungsvertrag. Ich möchte Dich vertraulich aufmerksam machen, dass unsere Ingenieure etwas Herausragendes in den Kächern haben: SunShineForever. Du kannst Dir plastisch vorstellen was darin steckt! Du wirst die erste sein, eine grosse Menge Muster kostenlos zu kriegen. Ich bitte Dich den Betrag von 100.000.- Schweizer Franken auf das Konto Nr. 222-1101.461.10 von der Bank ABC AG, in Basel CH zu überweisen.Ich hoffe Dir geholfen zu haben und verbleibe ich freundlichen Grüssen. Dein Bob, CEO

Found Hash: 1990800991
Strings mapping to that Hash:
1) Meine liebe Alice, ich bedanke mich vom Herzen für Deinen sehr willkommenen Auftrag. Ich möchte Deine Firma aufmerksam machen, dass unsere Ingenieure etwas Sensationelles in den Kächern halten : SunShineForever. Du kannst Dir vorstellen was darin steckt! Du wirst die erste sein, eine grosse Menge Fläschen gratis zu kriegen. Ich bitte Dich den Betrag von 100.000.- CHF auf das Konto mit der Nr. 222-1101.461.12 der Bank ABC AG, in Basel CH zu überweisen.Ich hoffe Dir geholfen zu haben und schliesse ich mit lieben Grüssen. Dein Bob, Geschäftsführer
2) liebe Alice, ich bedanke mich aufrichtig für Deinen erfreulichen Auftrag. Ich möchte Dich aufmerksam machen, dass unsere Ingenieure etwas Herausragendes in den Kächern halten : SunShineForever. Du kannst Dir plastisch vorstellen was darin steckt! Du wirst die einzige sein, eine grosse Menge Fläschen gratis zu erhalten. Ich bitte Dich die Summe von 100.000.- Schweizer Franken auf das Konto Nr. 222-1101.461.10 von der Bank ABC AG, 4001 Basel CH zu überweisen.Ich freue mich Dir geholfen zu haben und verbleibe ich freundlichen Grüssen. Bob, CEO

Found Hash: 252380
Strings mapping to that Hash:
1) Meine liebe Alice, ich bedanke mich aufrichtig für den erfreulichen Auftrag. Ich möchte Dich aufmerksam machen, dass wir etwas Herausragendes in den Kächern haben: SunShineForever. Du kannst Dir vorstellen was dahinten steckt! Du wirst die erste sein, eine grosse Menge Fläschen kostenlos zu kriegen. Ich bitte Dich den Betrag von 100.000.- CHF auf das

Konto Nr. 222-1101.461.12 von der Bank ABC AG, 4001 Basel CH zu überweisen.Ich hoffe Dir gedient zu haben und verbleibe ich freundlichen Grüssen. Bob, CEO
2) liebe Alice, ich bedanke mich aufrichtig für Deinen erfreulichen Auftrag. Ich möchte Dich vertraulich aufmerksam machen, dass wir etwas Herausragendes in den Kächern halten : SunShineForever. Du kannst Dir vorstellen was dahinten steckt! Du wirst die erste sein, eine ansehnliche Menge Muster kostenlos zu kriegen. Ich bitte Dich die Summe von 100.000.- CHF auf das Konto Nr. 222-1101.461.10 von der Bank ABC AG, in Basel CH zu überweisen.Ich freue mich Dir geholfen zu haben und schliesse ich freundlichen Grüssen. Bob, CEO

Found Hash: 1391400107
Strings mapping to that Hash:
1) Meine liebe Alice, ich bedanke mich aufrichtig für Deinen erfreulichen Lieferungsvertrag. Ich möchte Deine Firma vertraulich aufmerksam machen, dass wir etwas Sensationelles in den Reagenzgläsern haben: SunShineForever. Du kannst Dir plastisch denken was dahinten steckt! Du wirst die einzige sein, eine ansehnliche Menge Muster gratis zu kriegen. Ich bitte Dich die Summe von 100.000.- Schweizer Franken auf das Konto Nr. 222-1101.461.12 von der Bank ABC AG, in Basel CH zu überweisen.Ich hoffe Dir geholfen zu haben und schliesse ich freundlichen Grüssen. Dein Bob, Geschäftsführer
2) liebe Alice, ich bedanke mich aufrichtig für den sehr willkommenen Lieferungsvertrag. Ich möchte Dich vertraulich aufmerksam machen, dass wir etwas Sensationelles in den Reagenzgläsern haben: SunShineForever. Du kannst Dir plastisch vorstellen was darin steckt! Du wirst die einzige sein, eine ansehnliche Anzahl Muster gratis zu kriegen. Ich bitte Dich die Summe von 100.000.- Schweizer Franken auf das Konto Nr. 222-1101.461.10 der Bank ABC AG, 4001 Basel zu überweisen.Ich freue mich Dir geholfen zu haben und verbleibe ich mit lieben Grüssen. Dein Bob, Geschäftsführer

---