Applikationssicherheit Laboraufgabe 1

# Ressourcen

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

**original.txt**

Die originale Textnachricht von Bob, plaintext

**Patterns.txt**

Patterns, die benutzt werden, um eine Nachricht zu generieren, welche der Originalnachricht ähnlich sehen.

Die Form dazu ist die folgende:

* Je Pattern existiert eine Linie im File
  + Gesamthaft also 32 Linien => Bits in einem Integer
* Jede Linie ist durch eine Trennlinie, in diesem Fall „|“, unterteilt

Diese Patterns werden in der Klasse TextGenerator in ein 2D Array in der folgenden Form abgefüllt:

* Erster Index: Linie im File
* Zweiter Index: Position relativ zur Trennlinie => Links = 0, Rechts = 1

**Patterns\_Org.txt**

Gleich wie Patterns.txt.

# Klassen

**DESHash (hash)**

Allgemein: Durch diese Klasse kann ein Hashwert mittels DES generiert werden.

Detail:

1. Generiert den Initialisierungsvektor g0
2. Holt die Bytes vom übergebenen String
3. Speichert die Länge der aktuellen Nachricht in einer Variable zwischen
4. Überprüft, ob ein Padding nötig ist und fügt sie hinzu
   1. Länge wird nach der folgenden Formel berechnet: ((x/8)+1)\*8
   2. Padding in Form 1000….
5. Speichert die Länge der aktuellen Nachricht in dessen Byte Array
6. Erzeugt ein Objekt der Klasse PaddedBufferedBlockCipher
   1. Als Parameter wird ein Objekt der Klasse DESEngine übergeben
7. Iteration (von i bis Ende Nachricht; Schritt in BlockSize des Ciphers:
   1. Initialisiert den Cipher mit dem Schlüssel
   2. Erstellt ein Byte Array
      1. Als Grösse wird der OutputSize des Ciphers bzw. des DES genommen
   3. Cipher bearbeitet einen Block
   4. Cipher gibt den Output durch doFinal aus und speichert es im Block
   5. Erstellen des neuen Schlüssels
      1. Durch Formel
         1. Block muss in sich xor-en, da DES einen Output der Länge 2\*64 Bit liefert
8. Führt den letzten Schritt im DES aus. Berechnet also H in der Formel.
9. Wrapt das Ergebnis in ein ByteBuffer und form ein Integer daraus
10. Gibt diesen Integer als Resultat zurück

**Start (main)**

Allgemein: Diese Klasse ist ein Startpunkt für die Applikation.

Ansatz: Festes originales Dokument. Generiertes gefälschtes Dokument (mit n^32 Permutationen).

Detail:

1. Erzeugt Instanzen der Klassen TextGenerator und DESHash.
2. Ladet das File Patterns.txt
3. Erzeugt den Hashwert des originalen Textes
4. Schleife:
   1. Erzeugt den Hashwert der Kopie
   2. Prüft, ob die Hashwerte übereinstimmen
   3. Bricht ab, falls ein Hashwert gefunden wurde
5. Gibt den Informationen zur Kollision auf der Konsole aus

**StartPermutation**

Allgemein: Diese Klasse ist ein Startpunkt für die Applikation.

Ansatz: Beide Dokumente, sowohl gefälscht wie original, werden generiert (n^32 Permutationen je).

1. Festlegen, wie viele Kollisionen der Benutzer finden will
2. Instanzieren von je einem TextGenerator und einer HashMap für die Files
3. Instanzieren einer HashMap für di gefundenen Keys
4. Instanzieren der Klasse DESHash
5. Schleife; so lange bis der Zähler die gewünschte Anzahl Kollisionen erreicht hat:
   1. Generieren von je 2048 neuen Texten pro File und speichern dieser Texte inkl. deren Hashes in den zugeordneten HashMaps.
   2. Iterieren über die Keys der HashMap für die gefälschten Files
      1. Falls der Hash ebenfalls in der Map für die originales Files vorkommt
         1. Invariante: Falls der Hash bereits bekannt ist, ist mindestens ein originaler Text bekannt.
         2. Falls dieser Hash bereits bekannt ist
            1. Es soll überprüft werden, ob der Text zum Hash bereits abgespeichert wurde. Falls nicht, soll er abgespeichert werden.
            2. Falls der abgespeicherte Text einer der gefälschten Texte war, soll der Counter für gefundene Kollisionen hochgezählt werden.
         3. Falls dieser Hash nicht bekannt ist
            1. Es soll eine neue Liste kreiert und die Texte (sowohl gefälscht wie original) sollen mit dem dazu gehörenden Hash in der Map für gefundene Hashes abgespeichert werden.
6. Ausgeben der Kollisionen

**TextGenerator**

Allgemein: Diese Klasse generiert Kopien des Originals mit Permutationen.

Methodendetails:

loadTextFile: Diese Methode soll dazu dienen, die Patterns zu laden

1. Liest das File ein
   1. Dabei wird jede Linie einzeln eingelesen
   2. Jede Linie wird am Trennpunkt gesplitet und in einem 2D Array gespeichert
      1. 2D Array erster Index: Nummer der Linie
      2. 2D Array zweiter Index: Nummer des Patterns

getNextText: Diese Methode soll dazu dienen den nächsten Text aus dem 2D Array zu holen.

1. Überprüft, ob randomisiert werden soll
   1. Falls nicht, dann soll der nächste Text gemäss der Laufnummer ausgegeben werden
   2. Falls ja
      1. Den nächsten Integer aus dem Randomisierer holen.
      2. Überprüfen, ob diese bereits genommen wurde
         1. Falls ja, den nächsten Text ausgeben (sich selber aufrufen)
         2. Falls nicht, die Nummer in die Liste hinzufügen und den aktuellen Text ausgeben

getText: Diese Methode soll den Text anhand eines Integers generieren

1. Den Integer in dessen binärer Form in einen String konvertieren.
2. StringBuilder instanzieren
3. Durch diesen String iterieren:
   1. Der Index im String bestimmt die Linie bzw das Pattern
   2. Der Character (0,1) bestimmt, ob in einem Pattern die erste oder zweite Position genommen wird
   3. Append im StringBuilder
4. Rückgabe des Strings vom StringBuilder

# Klassenbeschrieb

**DESHash**

Hier wurde die DES-Funktion aus der Aufgabenstellung implementiert. Dabei wurden die Klassen DESEngine für den DES und PaddedBufferedBlockCipher, um die Engine in einer BlockCipher auszuführen, verwendet.

Es wurde grundsätzlich 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 müssen diese zwei Blöcke untereinander ein xor ausführen.

**TextGenerator**

Diese Klasse liest ein Patterns-File ein und generiert daraus Texte. Da ein Patterns-File genau 32 Möglichkeiten hat ein Text zu generieren, wurde 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.

**Start**

In dieser Klasse arbeitet die Applikation mit fixem originalen File und permutierender Kopie.

**StartPermutation**

In dieser Klasse arbeitet die Applikation sowohl mit permutierender Kopie als auch mit permutierendem originalem File.

# Ergebnisse

Es wurden zwei Varianten bzw. Interpretationsmöglichkeiten der Aufgabestellung implementiert.

Die einte Variante sieht vor, dass ein festes originales File vorhanden ist. Die Fälschungen werden anhand eines Pattern-Files generiert.

Als Startmethode wurde hier die Klasse Start genommen.

Diese Variante erzielte jedoch kein Ergebnis, auch wenn es über Nacht lief.

Die zweite Variante sieht vor, dass Originale, sowie Fälschungen anhand je eines Pattern-Files generiert werden.

Als Startmethode wurde hier die Klasse StartPermutation genommen und die gewünschte Anzahl Kollisionen in der Variable count angegeben.

Die Laufzeit betrug ca. 5 Minuten. Dies kann jedoch variieren.

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 Summe 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

--------------------------------------------