Michael Eckhardt
eckhar@hs-furtwangen.de

Gesamtanforderungen an das Kryptoprojekt

Anforderungen nach Projektbeschreibung

1. Framework mit Basisalgorithmen nach dem Baukastenprinzip

2. Lokal und Netzwerkfunktionalität
   es soll sowohl auf einem lokalen Rechner zu installieren sein, als auch von einem Server aufrufbar
   offene Frage: Sollen auch Verschlüsselungen/Entschlüsselungsszenarien (public/private Key) über Netzwerk möglich sein?

3. Programmiersprache Java oder C++

Anforderungen (vom 18.03.2010)

4. Schöne GUI
   übersichtlich, einfache Bedienung, erweiterbar (soll sich deutlich von Maple unterscheiden)

5. Plattformunabhängigkeit
   sollte mit Java gegeben sein

6. Anzeige von Zwischenergebnissen bei der Berechnung

7. Aufgabengenerierung
   aus einem Pool oder wirklich zufällig?, Klausurmodus

Anforderungen (vom 22.03.2010)

8. Multiple-Choice-Aufgaben
   als eine Art Wettkampf – lokal und über Netzwerk

9. Druck- und Textverarbeitungsfunktionalität zum dokumentieren

10. Angriffsszenarien auf die Verschlüsselung
    Kryptoanalyse – ggf. Möglichkeit eines Grids einbauen

11. Verschiedene Sprachpakete

12. Kryptoalgorithmen (z. B. DES, RSA, El-Gamal) und Basisalgorithmen als Blackbox
    sollen später aber auch nach dem Baukastenprinzip erstellbar sein (die Algorithmen müssen durch die vorhandenen Basisalgorithmen selbst zusammengeklickt werden, ggf. über eine Schwierigkeitsstufe einstellbar)

13. Ausgabe des Aufwandes der Berechnung für die Verschlüsselung und Entschlüsselung
    Zeitausgabe und ggf. Anzahl an Operationen

14. Einstellen der Verschlüsselungsstärke
    z. B. Bit-Länge des Schlüssels oder Anzahl der Runden

Anforderungen (vom 25.03.2010)

15. auf Grundfunktionalität beschränken
    am Anfang Wert auf Qualität, einfache Bedienung und Erweiterbarkeit legen
    mathematische Grundlagen reichen vorerst aus:

    i. Modulo, ggt, (erw.) Euklidische Algorithmus, Primzahltest, Hamming-Code, Statistik über Hammingcode, Eulersche Phi-Funktion, zyklische Codes, Square-and-Multiply

16. Erweiterbarkeit / Wiederverwendbarkeit (sehr wichtig)
    wie haben Schnittstellen auszusehen? (nachfolgende Semester sollen das Programm erweitern können)

17. Hilfefunktion
    entweder als reiner Text oder eine Art Video Tutorial mit Sprache (Flash-Video) oder nur Text

18. Exceptionbehandlung
    bei Eingabe falscher Parameter gibt es eine Fehlermeldung

Aufteilung

Mario Wieser

- Framework mit Basisalgorithmen nach dem Baukastenprinzip
- auf Grundfunktionalität beschränken
  am Anfang Wert auf Qualität, einfache Bedienung und Erweiterbarkeit legen
  mathematische Grundlagen reichen vorerst aus:
    i. Modulo, ggt, (erw.) Euklidische Algorithmus, Primzahltest, Hamming-Code, Statistik über Hammingcode, Eulersche Phi-Funktion, zyklische Codes, Square-and-Multiply
- Anzeige von Zwischenergebnissen bei der Berechnung
- Aufgabengenerierung
  aus einem Pool oder wirklich zufällig?, Klausurmodus
- Einstellen der Verschlüsselungsstärke
  z. B. Bit-Länge des Schlüssels oder Anzahl der Runden
- Ausgabe des Aufwandes der Berechnung für die Verschlüsselung und Entschlüsselung
  Zeitausgabe und ggf. Anzahl an Operationen

Philipp Stussak

- Plattformunabhängigkeit
  sollte mit Java gegeben sein
- Programmiersprache Java oder C++
- Schöne GUI
  übersichtlich, einfache Bedienung, erweiterbar (soll sich deutlich von Maple unterscheiden)
- Erweiterbarkeit / Wiederverwendbarkeit (sehr wichtig)
  wie haben Schnittstellen auszusehen? (nachfolgende Semester sollen das Programm erweitern können)
- Verschiedene Sprachpakete
- Multiple-Choice-Aufgaben
  als eine Art Wettkampf – lokal und über Netzwerk

Stefan Link

- Druck- und Textverarbeitungsfunktionalität zum dokumentieren

- Angriffsszenarien auf die Verschlüsselung
  Kryptoanalyse – ggf. Möglichkeit eines Grids einbauen

- Kryptoalgorithmen (z. B. DES, RSA, El-Gamal) und Basisalgorithmen als Blackbox
  sollen später aber auch nach dem Baukastenprinzip erstellbar sein (die Algorithmen müssen durch die vorhandenen Basisalgorithmen selbst zusammengeklickt werden, ggf. über eine Schwierigkeitsstufe einstellbar)

- Lokal und Netzwerkfunktionalität
  es soll sowohl auf einem lokalen Rechner zu installieren sein, als auch von einem Server aufrufbar
  offene Frage: Sollen auch Verschlüsselungen/Entschlüsselungsszenarien (public/private Key) über Netzwerk möglich sein?

- Hilfefunktion
  entweder als reiner Text oder eine Art Video Tutorial mit Sprache (Flash-Video) oder nur Text

- Exceptionbehandlung
  bei Eingabe falscher Parameter gibt es eine Fehlermeldung