

Aufgabe 5 Verschlüsselung

Die meisten Personal Computer verfügen heutzutage über unterschiedliche Netzwerk-Schnittstellen, die sowohl eine lokale Verbindung untereinander als auch eine über weite Entfernungen hinweg zulassen. So bietet beispielsweise ein Notebook mit Intel Centrino® Chipsatz dem Benutzer mobile Freiheit, indem es eine drahtlose Verbindung mit dem Internet ermöglicht. Die per Funk-signal übertragenen Daten können dabei prinzipiell von jedem empfangen werden und sollten daher geschützt, d.h. verschlüsselt übertragen werden. Auch zahlreiche Internet-Anwendungen erfordern eine gesicherte Datenübertragung, bei der die übertragenen Daten nicht von Dritten gelesen werden sollen, beispielsweise Produktbestellungen im Internet oder Online-Banking.



Blaise de Vigenère

Aufgabe 5a Verschlüsselungsverfahren

Das Bedürfnis der geheimen Übermittlung von Nachrichten existiert bereits seit langer Zeit. Bereits vor mehr als 2000 Jahren nutzte ein berühmter römischer Feldherr eine Methode zur Verschlüsselung, die nach ihm benannt wurde.

- Wie hieß dieser Römer und wie nennt man die nach ihm benannte Verschlüsselungsmethode?
- Beschreibe kurz das Prinzip, auf der diese Verschlüsselungsmethode beruht?
- Verschlüssele den Satz „*Es ist nicht wenig Zeit, die wir haben, sondern es ist viel Zeit, die wir nicht nutzen.*“ (Seneca) mit der gesuchten Verschlüsselungsmethode und benutze dabei ein Code-Alphabet, das mit dem Buchstaben „T“ startet.
- Entschlüssele den folgenden Satz: „Gsb rklox nso Obno xsmrd fyx excobox Ov-dobx qoobld, cyxnobx fyx excobox Usxnobx qovsorox.“
- Warum wird die Methode des Römers heutzutage nicht mehr benutzt?

Moderne Verschlüsselungsverfahren benutzen in der Regel so genannte Schlüssel, d.h. Geheimworte, um Daten zu verschlüsseln. Man unterscheidet zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren.

- Welches der beiden Verfahren wird bei der Verschlüsselung von E-Mails bevorzugt benutzt?
- Wieviele unterschiedliche Schlüssel werden bei der Verschlüsselung auf diese Art und Weise (z.B. bei Verwendung von PGP) von einer Person benötigt?
- Zu welchem Zweck (Ver- oder Entschlüsselung) wird welcher Schlüssel vom Sender bzw. Empfänger einer verschlüsselten E-Mail benutzt?

Aufgabe 5b Entschlüsselung eines Textes (Kryptoanalyse)

Der in Aufgabe 5a gesuchte Verschlüsselungsalgorithmus des Römers wurde im späten Mittelalter weiterentwickelt und ist heutzutage als Vigenère-Verschlüsselung bekannt. Der französische Diplomat und Kryptograph Blaise de Vigenère benutzte diese Methode zur sicheren diplomatischen Korrespondenz mit seiner Regierung.

- Beschreibe kurz mit eigenen Worten, wie sich die Vigenère-Verschlüsselung von der älteren Verschlüsselungsmethode unterscheidet.

Folgender englischer Text wurde mit Hilfe der Vigenère-Verschlüsselung chiffriert:

Boeizi jfibxp moeig kkf Wxxvz mswcerusb Kffnse Aysis psismejhoh kvo vrdsh gomi ft
ditvxscqcz bxsmo dmf b Rmj dbiuwmxzcxf tdeprfvc bbyae oc Qfcbij Zka jhkvxg dlrh
dvrbcmjhyv usxwzhi se wxxvubeksn gzfmyzhc hfilpvg kffid imsbc kky cvobw Kcnep
Wxxvz msehrslsc xf zoeu hri zbnyjhbc ufszzbq Qfcbij Zka kc srtfoejs pyeqdmfbkzhi eer
ziityvdoxgv oxh usmvvoci tccxj pbmeusrx ubsnhr xf wxhlgdvzsc affvhnwni

Hinweis: Leerzeichen sind bei der Kodierung ignoriert (übersprungen) worden.

- Entschlüssele den obigen Text. Erkläre dabei kurz die einzelnen Schritte Deiner Vorgehensweise. Wie lautet der dekodierte Text? Ergänze die fehlenden Satzzeichen!
- Wie lautet der Code-Schlüssel?

Hinweis: Der Code-Schlüssel ist der Name eines deutschen Flusses.

Aufgabe 5c Implementierung eines Zufallszahlengenerators

In verschiedenen Kryptographie-Verfahren werden Zufallszahlen zur Erzeugung von Code-Schlüsseln verwendet, um eine sichere Verschlüsselung zu gewährleisten. Eine sehr einfache Methode, eine Zufallszahl mit Hilfe einer getakteten Digitalschaltung zu erzeugen, ist die Benutzung eines linear rückgekoppelten Schieberegisters (Linear Feedback Shift Register, LFSR), siehe Abbildung.

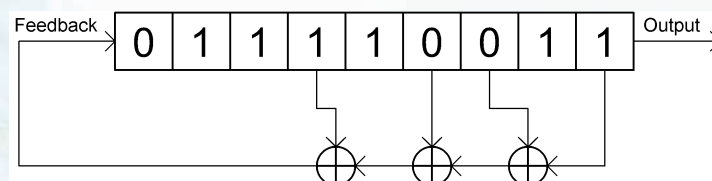


Bild eines LFSR mit 9 Registerbits, und 4 Rückkopplungspfaden bzw. 3 XOR-Gattern.

- Was zeichnet einen guten(!) Zufallszahlengenerator aus?
- Gibt es Startwerte, die für den oben gezeigten Zufallszahlengenerator **nicht** benutzt werden dürfen, damit er funktioniert, d.h. eine zufällige Folge von Nullen und Einsen generiert? Falls ja, welche? (Startwert ist der Wert, der bei einem Reset in die Speicherzellen/Register geladen wird.)

Entwerf eine möglichst einfache (digitale, getaktete) Schaltung, die eine zufällige Bit-Sequenz generiert. Die Bit-Sequenz soll sich nach jeweils 31 Takten wiederholen.

- Zeichne ein Blockschaltbild Deines Zufallszahlengenerators (ähnlich der oben gezeigten Abbildung des LFSR).
- Entwickle ausgehend von Deinem Blockschaltbild einen Schaltplan für die Schaltung, die aus Logikgattern und Registern besteht. Beschreibe kurz die Funktionsweise Deiner Schaltung.

Hinweis: Der benötigte Schaltungsteil zur Erzeugung von Taktsignal und Versorgungsspannung muss nicht gezeichnet werden, da er identisch mit dem aus Aufgabe 4c ist. Benötigte Taktsignale (clock, CLK) der verwendeten Bauteile bzw. Schaltplansymbole sollen im Schaltplan mit einer entsprechend benannten Signalleitung verbunden werden.

Bonusaufgabe (3 Punkte)

- Baue Deine Schaltung auf der mitgelieferten Steckplatine mit den im Bausatz enthaltenen Teilen auf und demonstriere ihre Funktion. Dokumentiere dies durch Fotos und/oder ein kurzes Video.

Viel Erfolg bei der fünften Aufgabe!

Falls Ihr Fragen zu den Aufgaben habt oder eine Hilfestellung benötigt, so schaut doch einfach mal in unser Forum: <http://www.unikik.uni-hannover.de/forum/>

Einsendeschluss: Sonntag, 15. Juni 2008, 23:59 (keine Verlängerung!).
Sendet Eure Lösungen per E-Mail an: aufgaben@intel-leibniz-challenge.de.

Die E-Mail sollte nicht größer als 3 MB sein (Die Dateien können gezippt sein)! Bitte gebt auch Euren Teamnamen, die Namen der Gruppenmitglieder sowie deren Schulen an. Bitte schreibt in der Betreffzeile der E-Mail Euren Gruppennamen und benennt Eure angehängten Dateien danach.

Ihr könnt/solltet Eure Lösung auch dann abgeben, wenn Ihr die letzte Teilaufgabe (die Profi-Aufgabe) nicht gelöst habt!

Die Teilnahmebedingungen und weitere Informationen findet Ihr unter:
<http://www.unikik.uni-hannover.de/ILC/>

Der Rechtsweg ist ausgeschlossen.