Kryptographie im Internet-Zeitalter

Es soll ein wirkungsvolles Verschlüsselungsprogramm entwickelt werden das in der Lage ist, einen frei wählbaren Text in ASCII - Format zu verschlüsseln. Der Verschlüsselungsvorgang darf nicht mehr rückverfolgbar sein d.h. rückrechnen vom Verschlüsselungsalgorithmus auf den Entschlüsselungsalgorithmus soll nicht möglich sein. Dieses Programm eignet sich hervorragend zum sicheren Verschicken von Nachrichten im INTERNET per EMAIL

Stefan Aichholzer, Betreuer: Edi Fleck DSK-536\\code

Analyse, Definition

Der Text wird in eine binäre Form gebracht und anschließend durch eine mathematische Formel verschlüsselt. In dieser Formel wird die Modulo-Operation verwendet. Dadurch wird unerwünschtes Entschlüsseln vermieden. In einem Durchgang werden jeweils 8 Bit verarbeitet. Diese Folge von 8 Bit langen Paketen nennt man Klartextvektoren. Diese Vektoren werden mittels einem Verschlüsselungsvektor verschlüsselt . Somit können die 8 Bit Pakete als Dezimalzahlen einfach und sicher weitergegeben werden. Bei der Entschlüsselung dieser Dezimalzahlen verwendet man einen Entschlüsselungsvektor, der diesen Prozeß rückgängig macht, und die binäre Information wieder verwendbar macht.

Anmerkung: Die Sicherheit wird um so größer, je größer die Vektoren gewählt werden.

Berechnete Vektoren

Ver- , Entschlüsselungsvektor,m,w,w^-1

Der Entschlüsselungsvektor darf frei gewählt werden, vorausgesetzt daß der nächst höhere Wert größer ist, als die Summe der vorhergegangenen Werte. e[n] > $\sum_{i=1}^{n} e[i]$

z.B. e = (3, 5, 10, 23, 45, 90, 179) ..... Entschlüsselungsvektor

Nun werden die 2 Ver- und Entschlüsselungsparameter (m, w) ermittelt. Sie dürfen ebenfalls frei gewählt werden. Voraussetzungen: m > $\sum_{i=1}^{n} e[i]$, m und w müssen den größten gemeinsamen Teiler von 1 haben. z.B. m=391 w=81

Der Verschlüsselungsvektor wird durch a[i] = (e[i] * w)*) mod m ermittelt. Dieser Vektor darf auch öffentlich bekanntgegeben werden. Die Modulo-Operation verhindert das Rückrechnen auf den Entschlüsselungsvektor. (Falltürprinzip d.h. diese Rechnung ist nur in eine Richtung möglich) z.B. a =(243, 14, 28, 292, 126, 252, 32) Verschlüsselungsvektor

Der hier verwendete Index „i“ z.B. a[i] steht für die Position im Vektor a[2] wäre in diesem Fall 14. Verschlüsseln:

C= x[i]*a[i] $\sum_{i=0}^{n} x[i] * a[i]$

x ist die Bezeichnung des Klartextvektors z.B. (0,0,1,0,1,1,1,0). Hier steht in binärer Form der ASCII Wert des Zeichens das verschlüsselt wird.

C ist nun eine Dezimalzahl und kann verschickt werden. D= C * w^-1 mod m

w^-1 = $\frac{y.m+1}{w}$ (In diesem Fall wäre w^-1=140 und y=29)

w^-1 und y sind Parameter die einfach berechnet werden können. „y“ soll so gewählt werden, damit w^-1 ganzzahlig ist.

D = x[i] * e[i] $\sum_{i=0}^{n} x[i] * e[i]$ Hier wird der Klartextvektor x wieder verwendbar

Verschlüsseln

Der Computer liest aus der Quelldatei die Zeichen ein . Der Dezimalwert des Zeichens muß als „unsigned char“ definiert sein (wegen der Sonderzeichen z.B. ü, ö, ß, °,...). Dieser Wert wird in einen 8-stelligen Binärcode umgerechnet. z.B. Feld ={0,1,1,0,0,1,0,1}. Aus diesem Code errechnet der Computer C mit C=x[i]*a[i]; Dieser Wert wird anschließend auf die Zieldatei geschrieben.

Entschlüsseln

Der Entschlüsselungsvorgang gleicht weitgehend dem Verschlüsselungsvorgang. Der Computer liest aus der Quelldatei die C-Werte ein. Anschließend ermittelt er D mit D=C*w^-1 mod m. Dieser Wert wird mit Hilfe des Entschlüsselungsvektors wieder in binäre Form gebracht und in einen Dezimalwert umgerechnet. Dieser Dezimalwert entspricht dem ASCII-Code des Zeichen das in die Zieldatei geschrieben wird.

Verschlüsselungsprogramm

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

void Eingabe(char ziel[ ],char quell[ ]);

void Eingabe(char ziel[ ],char quell[ ])
{ clrscr();
  printf("Bitte geben sie den Pfad und Dateinamen des Reintextes
ein:\n");
  printf("Pfad=");
  scanf("%40s",quell);
  printf("Bitte geben sie den Zielpfad des verschlüsselten Textes
ein:\n");
  printf("Pfad=");
  scanf("%40s",ziel);
}
void main ()
{ unsigned char hilf,hilf2;
  int Feld[8],C,k,i;
  int a[8]={243,405,79,401,721,711,610,651};
  /* Anstelle der vorgegebenen Werte kann auch
     eine Eingabe der Werte erfolgen Sicherheit */
  char Zeichen,Quell[30],Ziel[30];
  FILE *Datei;
  FILE *Output;
  Eingabe(Ziel,Quell);
  Datei=fopen (Quell,"rt");
  Output=fopen (Ziel,"w+");
  do
  { Zeichen=fgetc(Datei);
    hilf2=Zeichen;
    for(k=128,i=0;i<=7;i++)
    { hilf=hilf2/k;
      if (hilf>=1)
      { Feld[i]=1;
        hilf2=hilf2-k;
      }
      else
      Feld[i]=0;
      k=k/2;
    }
    C=0;
    for (i=0;i<=7;i++)
    { C=C+(Feld[i]*a[i]);
    }
    fprintf(Output,"%d\n",C);
  }
  while (Zeichen != EOF);
  fcloseall();
}
```

Anmerkung: Das Entschlüsselungsprogramm finden Sie auf Diskette 536