Dokumentation.Pseudozufallsgenerator

Aufgabe.

Ziel ist es einen „zufälligen“ Schlüssel zu erzeugen, der unendlich lang werden kann, um unbeschränkt große Bitanzahlen zu verschlüsseln.

Vorgehensweise.

Der Generator erstellt den Schlüssel mit Hilfe des Eingabewertes, den sog. Seed. Alle Werte des Schlüssels entstehen durch ihn und sind dadurch von diesem abhängig und überhaupt nicht zufällig. Diese mathematische Grundlage bietet der lineare Konguenzgenerator.

Linearer Konguenzgenerator.

$$x_i = \big((x_{i-1} \cdot a\ ) + c\big)\%\ 2^n$$

x_i ist ein neuer „Zufallswert“, der dem Schlüssel zugeordnet wird.

x_{i-1} ist dementsprechend der vorherige Wert, der bestimmt wurde.

Da jeder Wert aus der Menge aller x_i erst durch einen vorherigen Wert entsteht, muss es einen Startwert geben: $x_0 = seed$.

n sei aus $\mathbb{N}$ und markiert die Bitintervallgrenze in der x_i liegt. Intervall: $[0, n]$.

c sei aus $\mathbb{N} < 2^n$ und dient als Summand.

a sei in $\mathbb{N} < 2^n$ und dienst als Multiplikator.

Entstehung des Schlüssels.

Natürlich erkennt man schnell, dass durch mehrere bekannten Werte aus der Menge der x_i und ein wenig geschickte Mathematik alle Parameter und damit auch der $seed$ gefunden werden können. Um dem aus dem Weg zu gehen, wird dem Schlüssel nur die rechte Bithälfte von jedem Wert x_i zugeordnet. Der Generator arbeitet jedoch mit dem ganzen Werten von x_i weiter. Beispiel:

$$x_i = 1001\ 1111$$

$$x_s = 1111$$

Der Schlüssel s besteht demnach aus allen x_s, die aneinandergereiht werden.

$$s = x_{s1}\ , x_{s2}, x_{s3}, \ldots$$

Abschneiden der linken Bithälfte.

Der Wert von x_s entsteht durch eine Art Maske oder Folie, die über x_i gelegt wird. Diese ist so aufgebaut, dass durch sie nur die rechte Bitseite von x_i durchschimmert und x_s zugeordnet wird. Im Programm wird mit dem Vergleichsinstrument „&" gearbeitet. Es werden die Bits von der Maske mit den der von x_i verglichen. Wenn beide an der gleichen Stelle den gleichen Bitwert haben, wird dieser übernommen, ist dies nicht der Fall gilt für x_s an der Stelle 0. Um nur die rechte Seite zu übernehmen, muss also eine gleichlange Bitmaske m erzeugt werden, die von links bis zur Mitte aus Nullen und von der Mitte bis rechts aus Einsen besteht.

Beispiel:

$$x_i = 1111\ 1001$$

$$m = 0000\ 1111$$

$$x_s = 0000\ 1001$$

Pseudozufallsgenerator als Klasse.

Der Generator wird als Klasse erzeugt. Als Eingabe bekommt er die Parameter $a, b, (n?)$ und den $seed$. Der Vorteil an einer Klasse ist, dass jeder letzte Wert von x_i gespeichert wird. Sodass man innerhalb der Klasse mit Hilfe einer Methode jeden nächsten Teilschlüssel k_i mit der Bitanzahl n erzeugen kann. Und die Möglichkeit besteht den zusammengesetzten Schlüssel k aus den Teilschlüsseln k_i unbeschränkt lang zu wählen.