Exemple. **Insuffisance de PRNG.** — Un Exemple d'Attaque.

Supposons que $\begin{cases} S_0 = \text{base} \\ S_{i+1} = A S_i + B \pmod m, \quad i \geq 0. \end{cases}$

où $|m|_2 \sim 100$ bits, $S_i, A, B \in \{0, 1, \dots, m-1\}$.

module m public ; (A, B) secret (avec éventuellement S_0),

$\Rightarrow$ taille de la clé $\sim$ 200 bits.

suffisant contre une attaque exhaustive

Alice peut chiffrer selon la figure précédente.

$y_i = x_i + \Delta_i \pmod 2$ où Δ_i fait partie des bits représentant un certain S_j.

- Hypothèse : O sait que x contient 300 bits de clair et bien sûr le chiffré. O peut calculer les 300 bits de la S-clé :

$$\Delta_i = y_i + x_i \pmod m \quad i = 1, \dots, 300.$$

D'où O connaît : $S_1 = (\Delta_1 \cdots \Delta_{100})$, $S_2 = (\Delta_{101} \cdots \Delta_{200})$,

et $S_3 = (\Delta_{200} \cdots \Delta_{300})$. Je peut écrire :

$$\left\{ \begin{array}{l} S_2 \equiv A S_1 + B \pmod m \\ S_3 = A S_2 + B \pmod m. \end{array} \right\} \text{ O inconnus } A, B \text{ sur } \mathbb{Z}_m.$$

D'où $\begin{cases} A \equiv (S_2 - S_3)/(S_1 - S_2) \pmod m. \\ B \equiv S_2 - S_1 (S_2 - S_3)/(S_1 - S_2) \pmod m. \end{cases}$

Si $\text{pgcd}(S_1 - S_2, m) \neq 1$, plusieurs solutions, et

O peut trouver A, B en utilisant quelques bits du ~~chiffré~~ clair ou par essais de cryptage $\square$