$\ell(n)$ biți cei mai puțini semnificativi $\Rightarrow$ seed de generează cheia pr.

(plec de la x_0, e, generez x_1 $\rightarrow$ iau cei mai puțini semnif. biți din x_1, generez x_2 și iau cei mai puțini semnif biți din x_2 $\dashrightarrow$ repet cheia pr.)

$(x_1)_{\ell(n)}$ $(x_2)_{\ell(n)}$.

Complexitate a RSA_{gen}: $(\log N)^3$

Schemeu.

$\mathcal{G}(1^n)$: $k \leftarrow \mathcal{G}(1^n)$

$\mathcal{E}(k,m)$ $|m| = \ell(n) > n$

$G(k)$, set $c = G(k) \oplus m$ (XOR).

decriptare: $\mathcal{D}_{(k,c)}$ se procedează identic: se calculează

$m = G(k) \oplus c$.

→ în cadrul criptosistemelor pr, cheia de criptare se schimbată de la mesaj la mesaj —

$m_1 \dashrightarrow c_1 = m_1 \oplus G(k)$

$m_2 \dashrightarrow c_2 = m_2 \oplus G(k)$

$c_1 \oplus c_2 = m_1 \oplus m_2$ → se obține cu aprox. 1 bună (m_1, m_2)

- ele sunt foarte rapide în practică
- A 2-a clasă de cript. - cu cheie din:

Criptosistemele bloc = mesajul m e împărțit în blocuri de mesaj și criptarea se face bloc cu bloc.