



schema pentru o rundă

runda 8.5

Algoritm generare subchei:

- **Cheia inițială de 128 biți se împarte în 8 subchei** (acestea vor fi primele 8 subchei folosite în algoritm)
- După ce am folosit **toate** (atenție, nicio subcheie nu se pierde!!!) cele 8 subchei, pentru a genera subcheile în continuare, **cheia inițială se rotește la stânga cu 25** și se împarte din nou în 8 subchei ș.a.m.d
- Total 52 subchei (6 subchei x 8 runde + 4 subchei din ultima rundă)



Adunare modulo 2^{16} (65536)



xor



Înmulțire modulo $2^{16} + 1$ (65537)