(4.2) one-time Pad (OTP)

Un cryptosystème est sûr inconditionnellement s'il ne peut être cassé même avec une infinité de Ressources calculatoires.

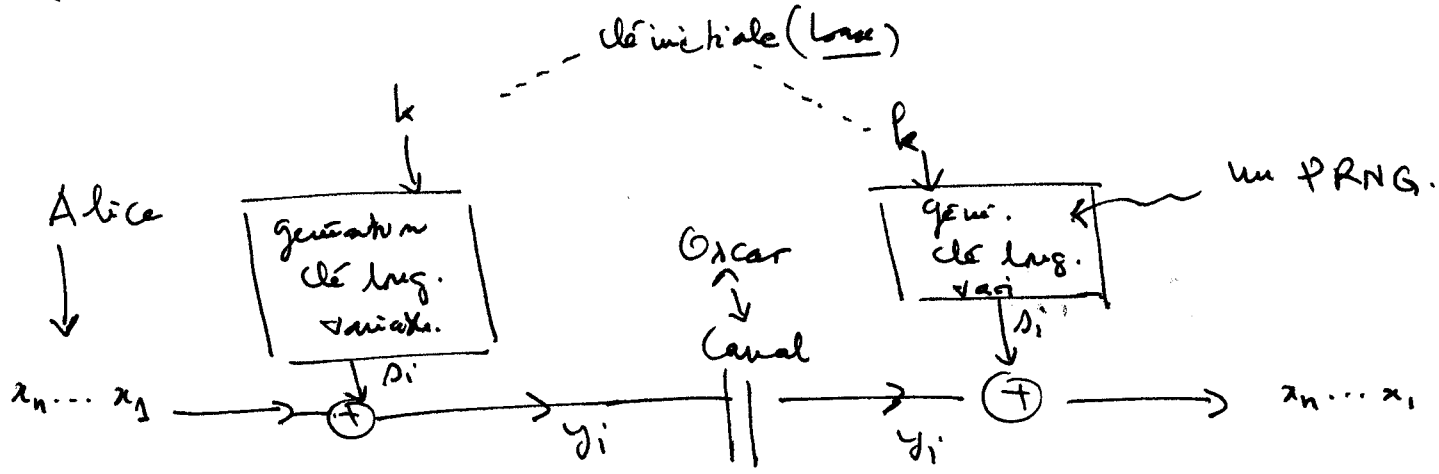
L'exemple est

OTP:

1. k_i est engendré par un TRNG.
2. La clé est connue que de A et B.
3. chaque k_i est utilisé une seule fois

Sûr mais impratiquable : $\log(\text{clé}) = \log(\text{texte})$.

(4.3). Vers le n-cryptage pratique.



- **Def.** Un cryptosystème est calculatoirement sécurisé si le meilleur algorithme connu pour le casser exige t opérations.
- Utilisant une clé k connue par A et B ($\sim$ 100 bits), et on utilise un PRNG pour engendrer (k_i) avec k base.