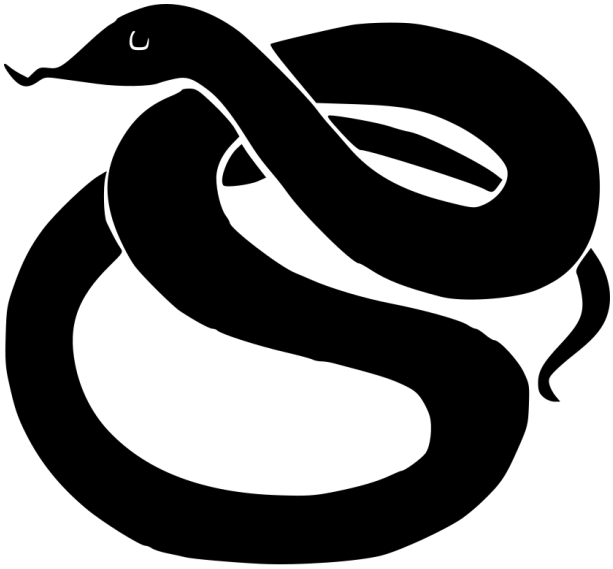
Algorithme de chiffrement par bloc : Serpent

Rapport

NGUYEN Alexandre - MILLOT Nathan



Licence Informatique TREC 7 Semestre 6

Date : 26 septembre 2025

Table des matières

Espaces de définition

1 Messages en clair et chiffrés

L'algorithme Serpent est un chiffrement par bloc avec :

— Espace des messages en clair $M = \{0,1\}^{128}$;

— Espace des messages chiffrés $C = \{0,1\}^{128}$.

Chaque bloc est donc constitué de 128 bits.

2 Clés

L'espace des clés dépend de la taille choisie :

— $K = \{0,1\}^{128}$;

— $K = \{0,1\}^{192}$;

— $K = \{0,1\}^{256}$.

En pratique, Serpent est défini pour ces trois tailles de clé.

Description du schéma Serpent

1 Structure générale

Serpent est basé sur un **réseau de substitution-permutation (SPN)**. Il comporte 32 rondes successives :

1. Ajout de sous-clé (XOR avec la sous-clé de ronde) ;
2. Substitution via une des 8 S-boxes (non-linéarité) ;
3. Transformation linéaire (permutation de bits).

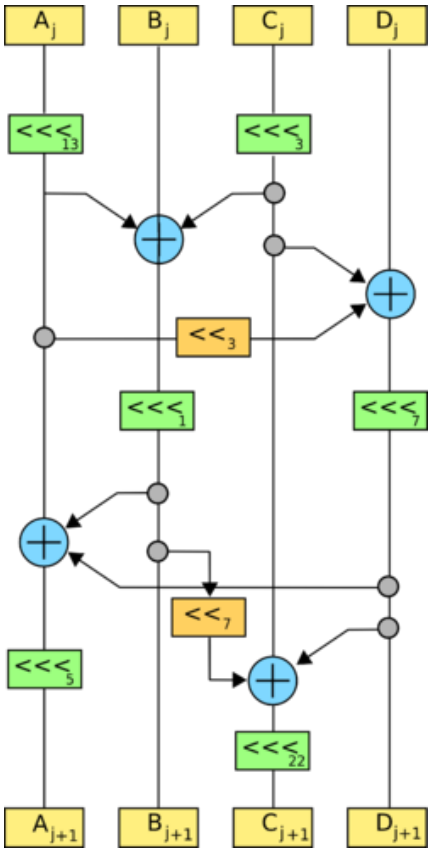


FIGURE 1 – Schéma général de Serpent

2 Sous-fonctions

Génération de sous-clés

À partir de la clé initiale, Serpent dérive 33 sous-clés de 128 bits chacune, notées $K_0, K_1, \ldots, K_{32}$.

Substitution (S-boxes)

Huit S-boxes différentes sont utilisées, notées $S_0, \ldots, S_7$. Elles transforment des blocs de 4 bits en 4 bits, et sont choisies de manière cyclique au fil des rondes.

Transformation linéaire

Chaque ronde applique une permutation fixe des bits pour assurer une bonne diffusion.

Dernière ronde

La dernière ronde est légèrement différente : après la substitution, il n'y a pas de transformation linéaire, seulement l'ajout de sous-clé.

Exemple d'application

Un cas concret d'utilisation de Serpent est son intégration dans certains logiciels de chiffrement comme **TrueCrypt** (ancien logiciel de chiffrement de disque), où il était proposé comme alternative à AES. Ce type d'application illustre bien l'usage de Serpent dans la protection des données sensibles stockées localement.

Sécurité et limites

1 Résistance aux attaques

Serpent a été conçu avec une marge de sécurité très élevée :

— Résistant à la cryptanalyse différentielle et linéaire ;

— Résistant aux attaques par clé liée.

Ses 32 rondes sont considérées comme surdimensionnées par rapport au minimum nécessaire (16–24 rondes auraient suffi).

2 Limites actuelles

Malgré sa robustesse, Serpent n'a pas été choisi comme AES en raison de sa relative lenteur par rapport à Rijndael (AES). Aujourd'hui, il est toujours considéré comme sûr, mais il est moins utilisé que AES ou ChaCha20, qui sont devenus les standards de fait.

Conclusion

Serpent est un algorithme de chiffrement robuste et bien conçu, qui mise sur la prudence et la sécurité. S'il n'a pas été choisi comme AES, il reste un chiffrement respecté, encore pertinent pour l'enseignement et certaines applications pratiques.