

De la Cryptographie à la Sécurité

Serge Vaudenay

<http://lasecwww.epfl.ch/>



ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

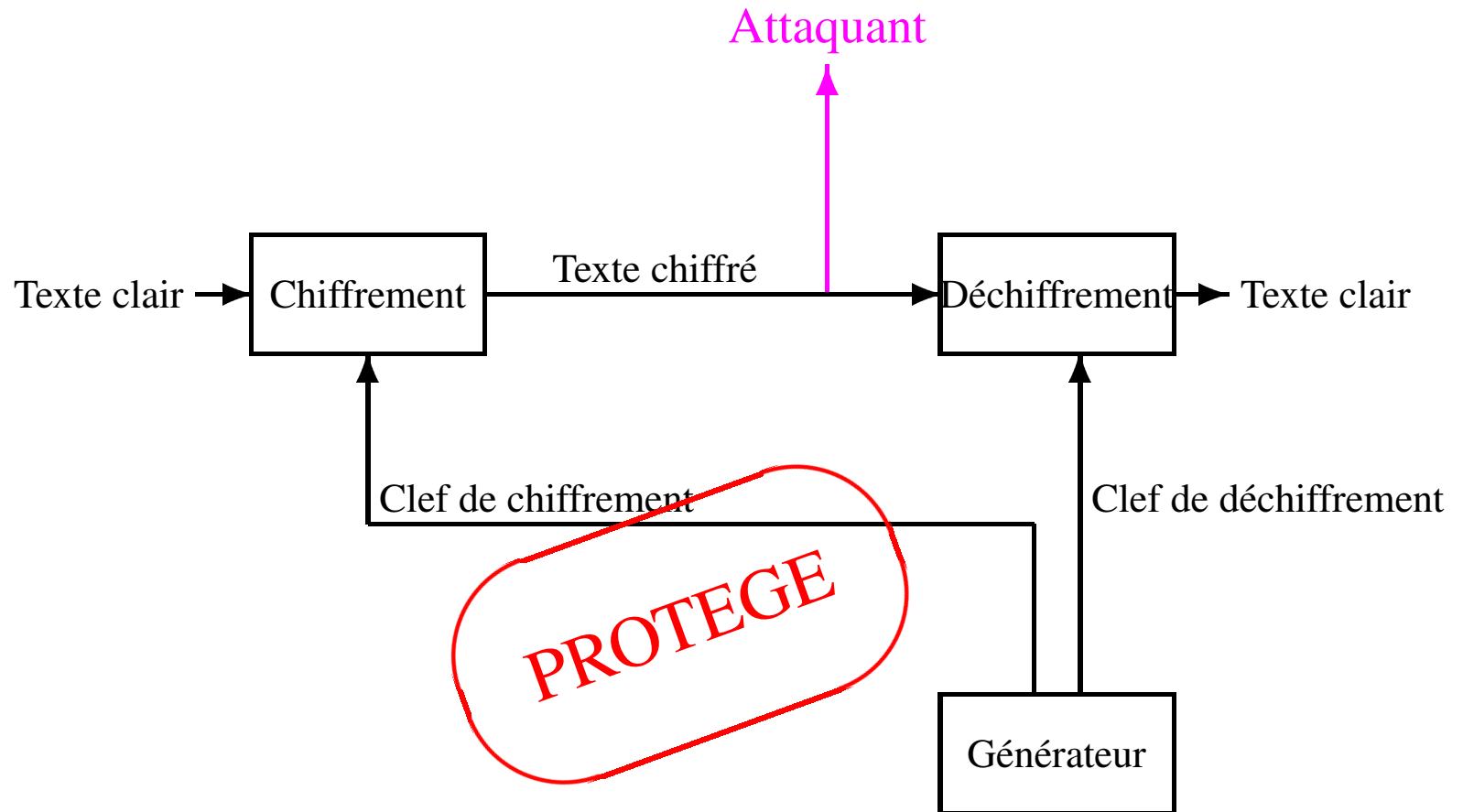
Sommaire

- ★ La cryptographie en théorie
 - chiffrement RC5
 - mode CBC
 - chiffrement RSA
- ★ Deux cas d'échecs de la cryptographie
 - des nombres entiers dans la vraie vie
 - des messages numériques dans la vraie vie
- ★ Conclusion

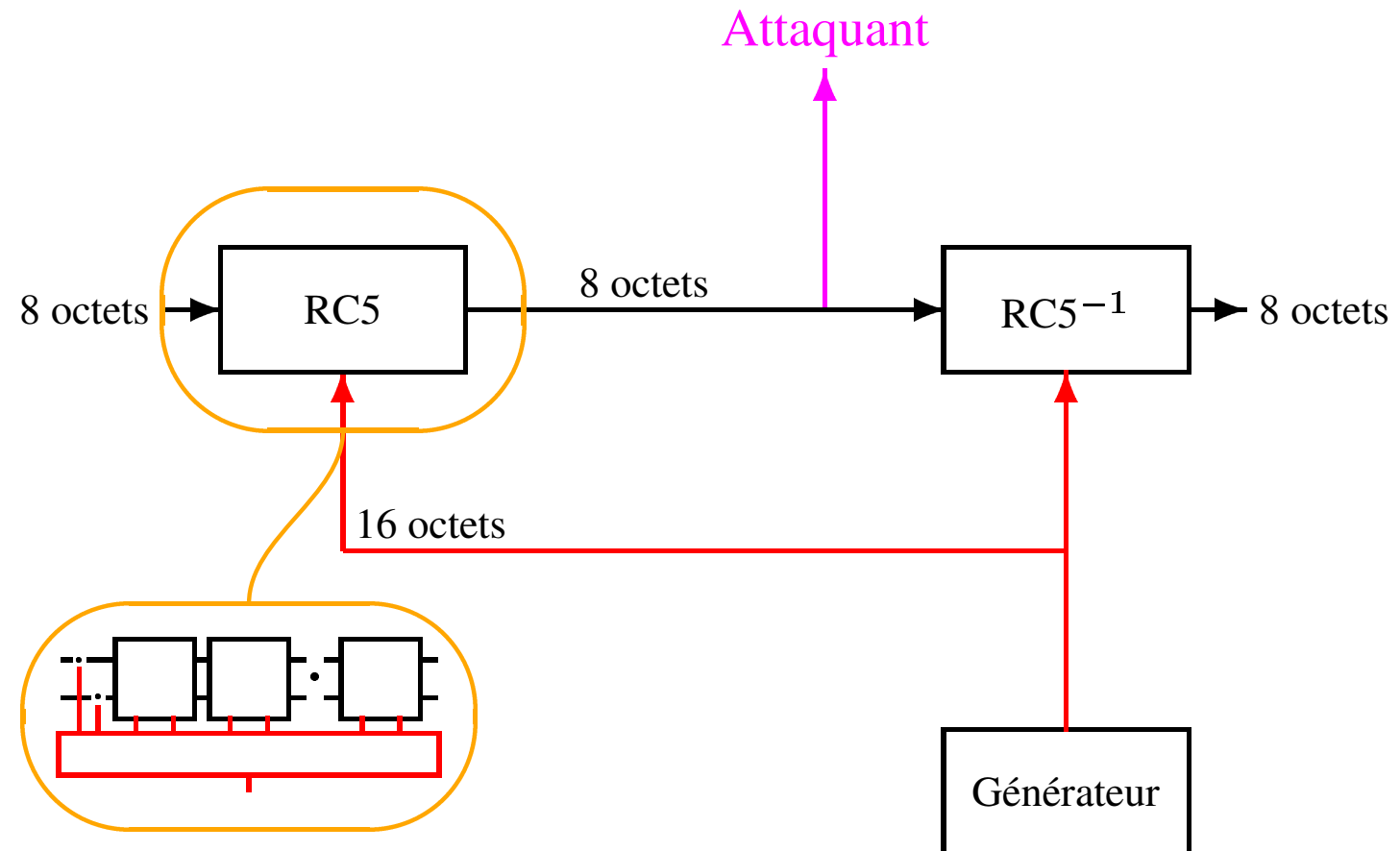
La sécurité des communications

- ★ Confidentialité
- ★ Intégrité
- ★ Authentification
- ★ Fiabilité
- ★ Protection de la vie privée
- ★ ...

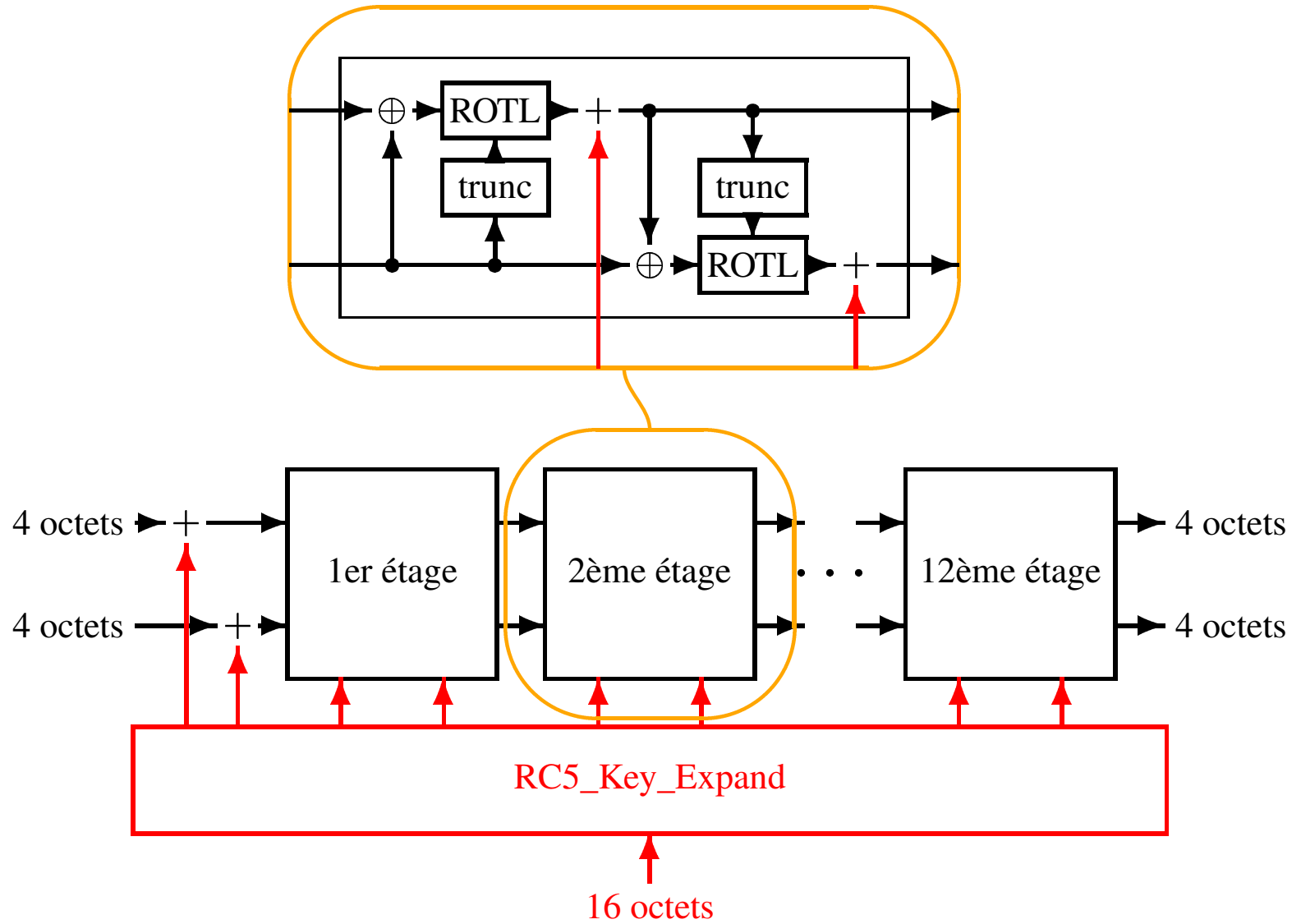
Confidentialité: le chiffrement



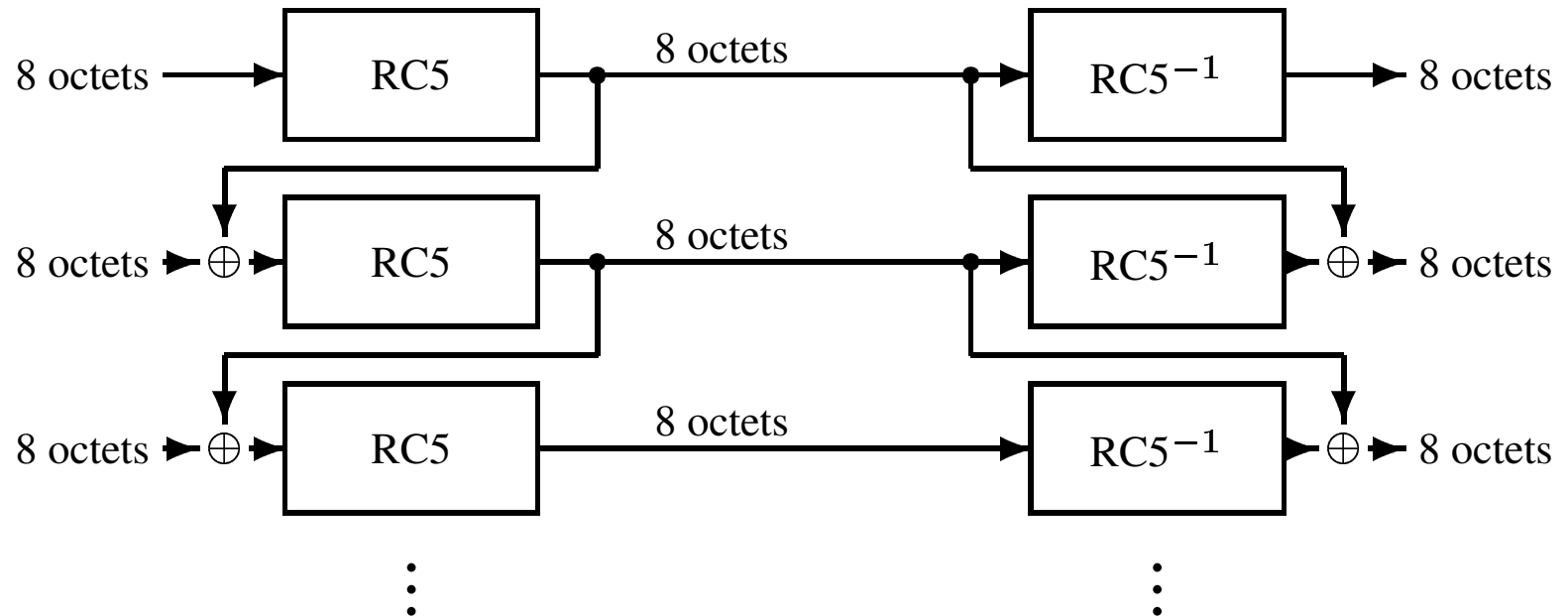
Chiffrement par blocs RC5



RC5

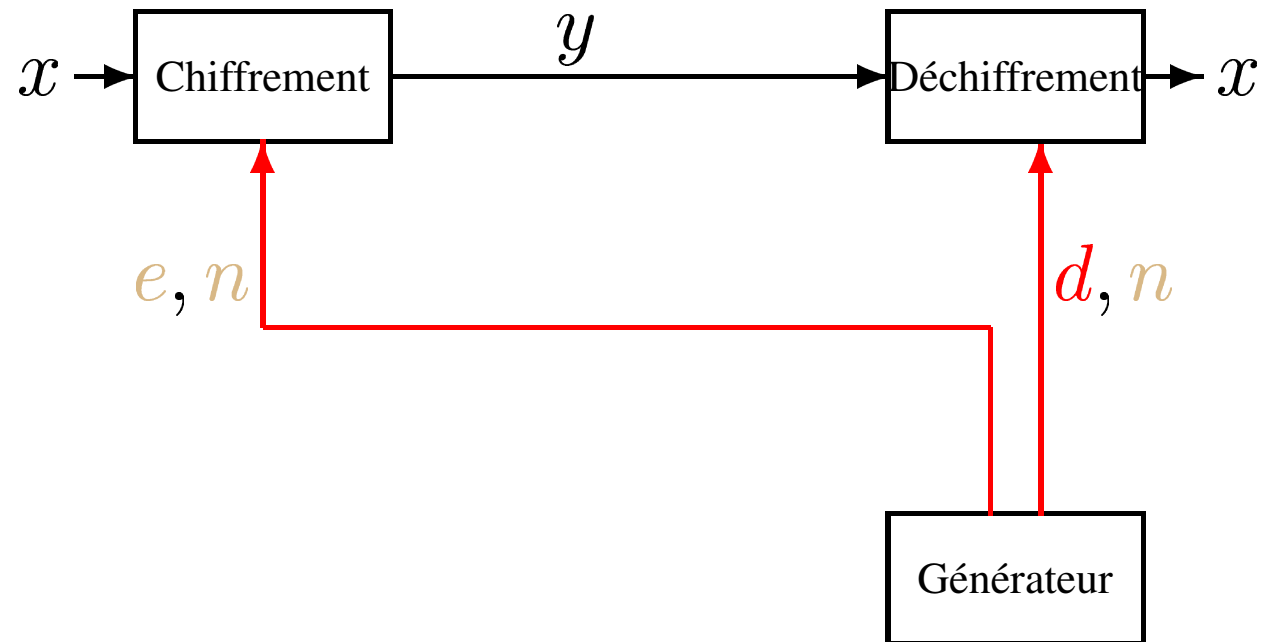


Mode opératoire CBC



- ★ RC5 chiffre un bloc de 8 octets
- ★ RC5-CBC chiffre un flux de blocs de 8 octets

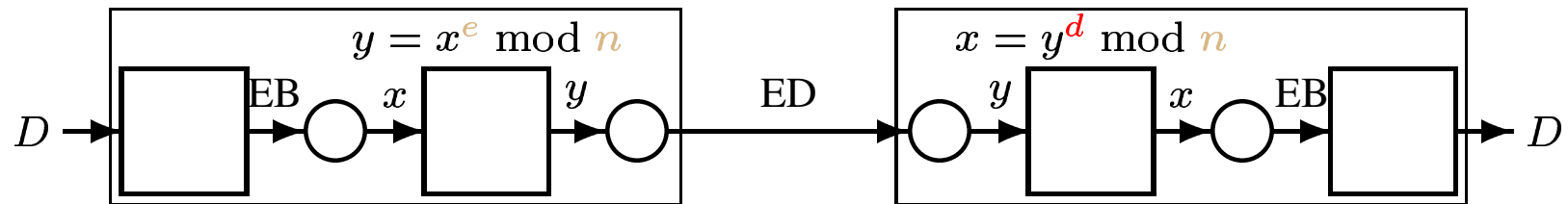
Chiffrement RSA



- ★ $n = p \cdot q, \quad e \cdot d \bmod (p - 1)(q - 1) = 1$
- ★ $y = x^e \bmod n$
- ★ $x = y^d \bmod n$

Des Nombres Entiers dans la Vraie Vie

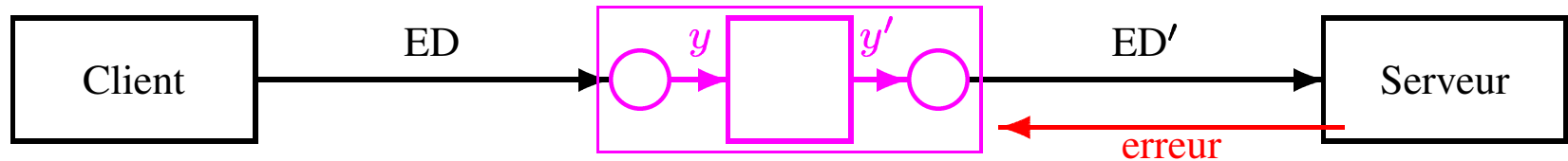
Chiffrement PKCS#1



- ★ D : au plus $k - 11$ octets (ex: $k = 128$)
- ★ EB: $00\ 02 || PS || 00 || D$ (k octets)
- ★ PS: *Padding String*, octets aléatoires ($\neq 00$)

- ★ que faire si EB n'est pas au format?

Attaque de Bleichenbacher



$$y' = s^e \cdot y \bmod n$$

- ★ si le serveur accepte, alors $(y')^d \bmod n$ est de la forme $00\ 02\|\dots$
- ★ donc $2 \times 256^{k-2} \leq s \cdot x \bmod n < 3 \times 256^{k-2}$
- ★ avec 1 000 000 tentatives, on peut reconstituer x !

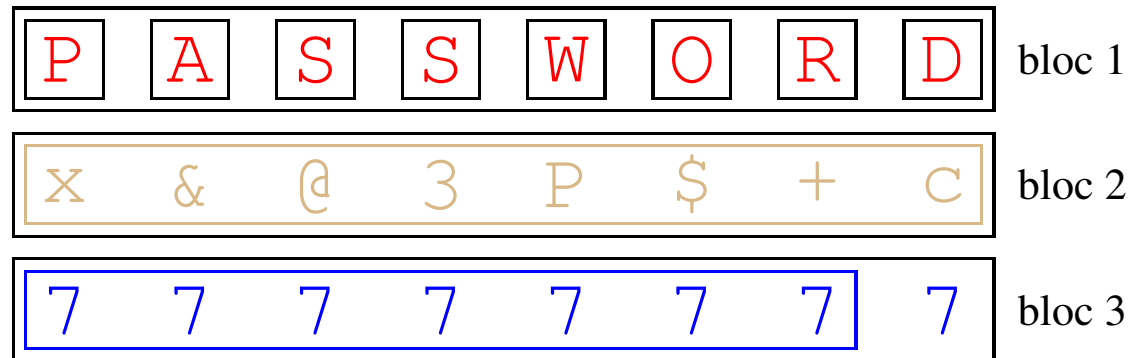
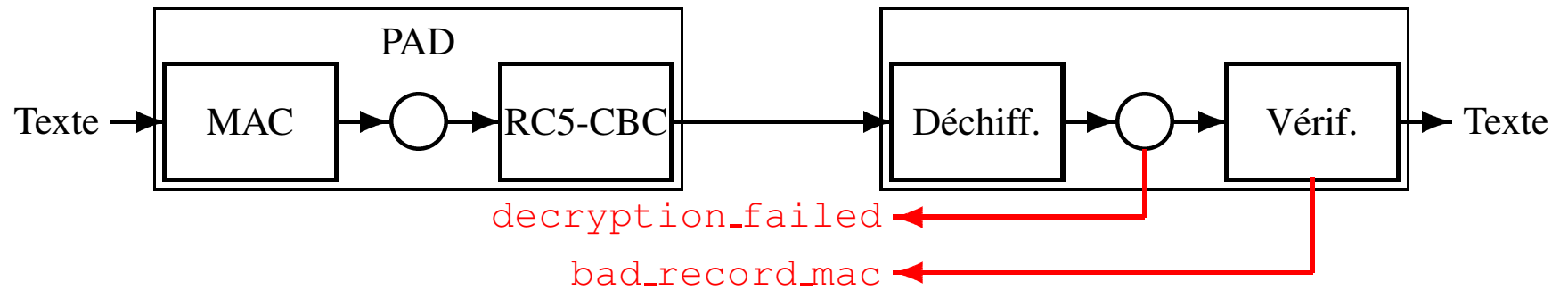
Moralité

Problèmes de standardisation

- ★ l'abus de maths nuit gravement à la sécurité
- ★ conversions de types: ne pas introduire de vulnérabilité

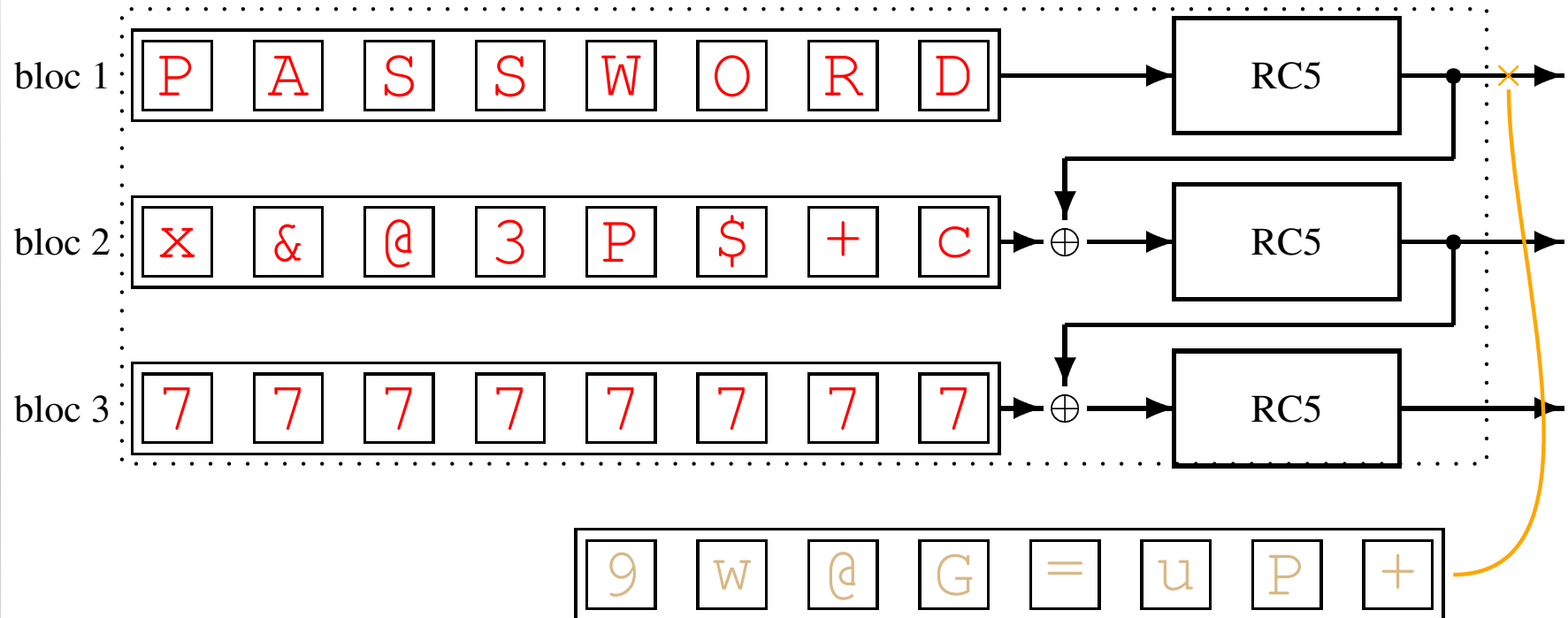
Des Messages Numériques dans la Vraie Vie

CBCPAD dans TLS

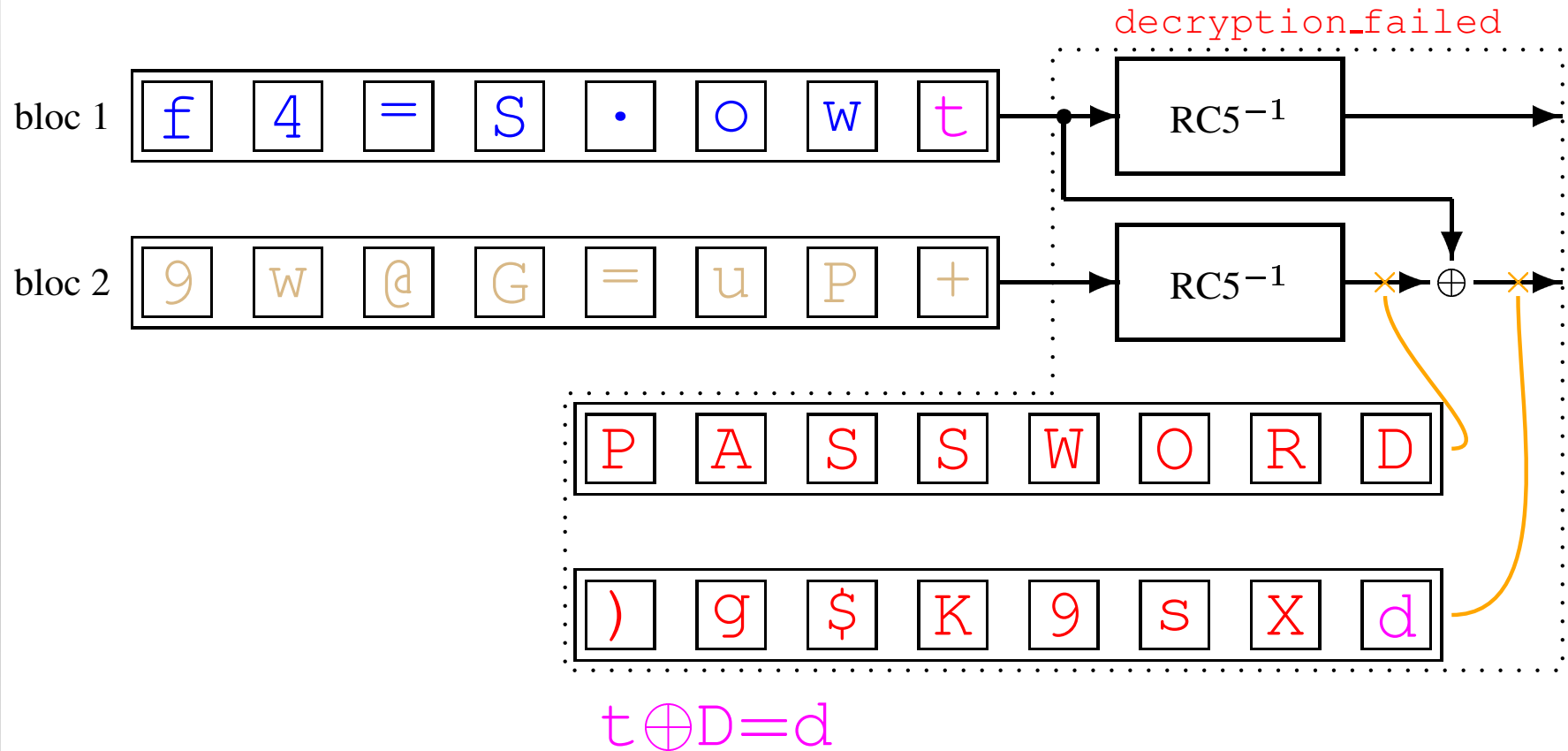


si le dernier octet est égal à n , vérifie que le message se termine par $n + 1$ octets égaux à n

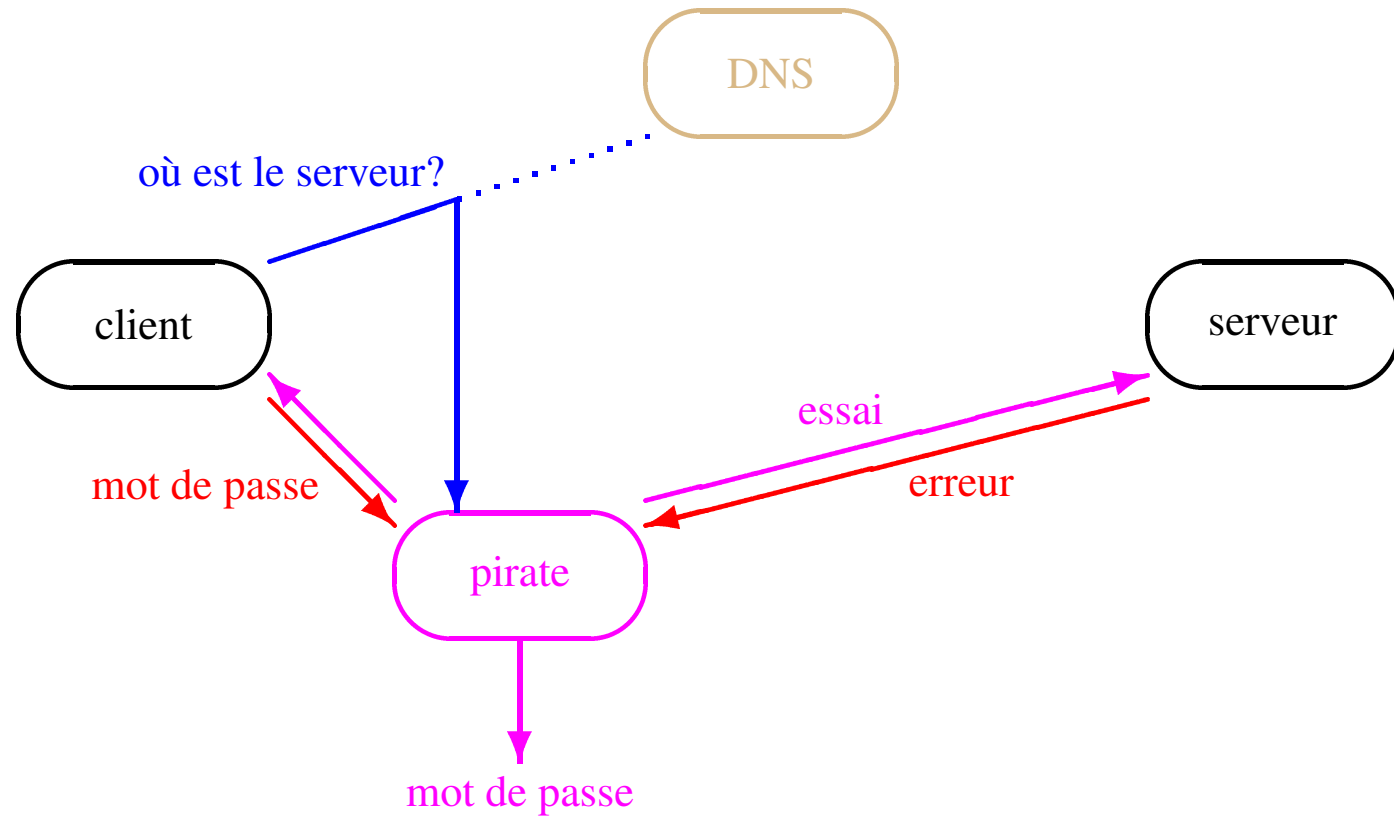
Chiffrement CBCPAD



Déchiffrement CBCPAD



Attaque contre TLS



Mise en œuvre

- ★ ça marche contre WTLS!
- ★ ça ne marche pas contre TLS!
- ★ la session est coupée après une erreur
- ★ les erreurs sont chiffrées

Moralité

Problèmes de standardisation

- ★ l'abus d'informatique nuit gravement à la sécurité
- ★ problèmes de *padding*: ne pas introduire de vulnérabilité

Conclusion

- ★ avant
- ★ après
- ★ il y a encore du travail!