CRYPTOGRAPHIE

Modes opératoires

E. Bresson

SGDN/DCSSI
Laboratoire de cryptographie

Emmanuel.Bresson@sgdn.gouv.fr

I. CHIFFREMENT SYMÉTRIQUE

I.1. MODES OPÉRATOIRES

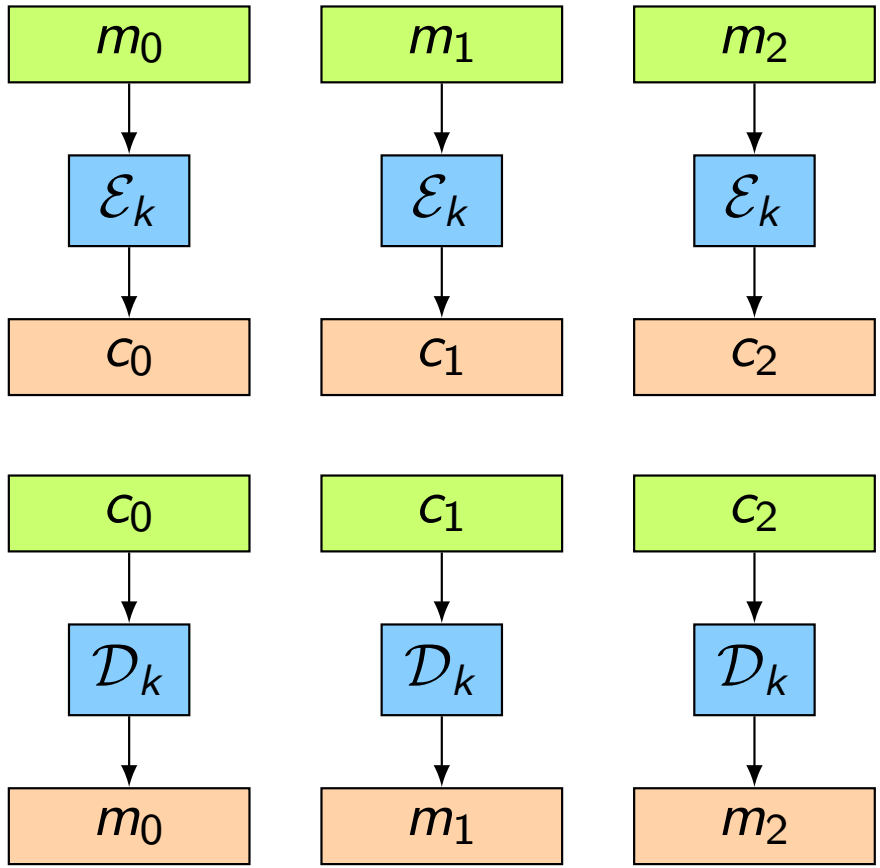
Organisation de la section « MODES OPÉRATOIRES »

Modes de chiffrements

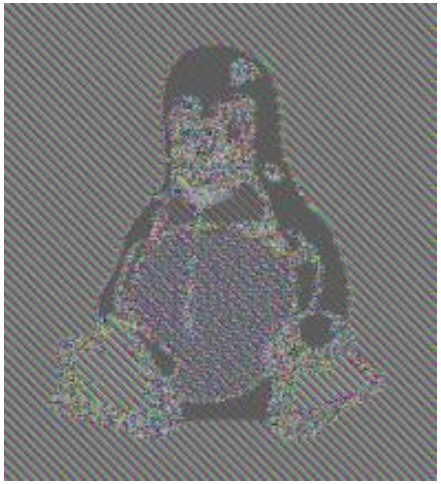
MODES OPÉRATOIRES: ECB

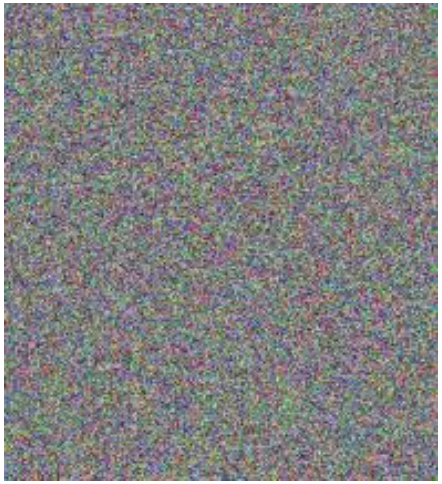
Chiffrement de messages plus longs que 128 bits. . .

Mode ECB (*Electronic Code Book*) deux blocs identiques sont chiffrés de manière identique

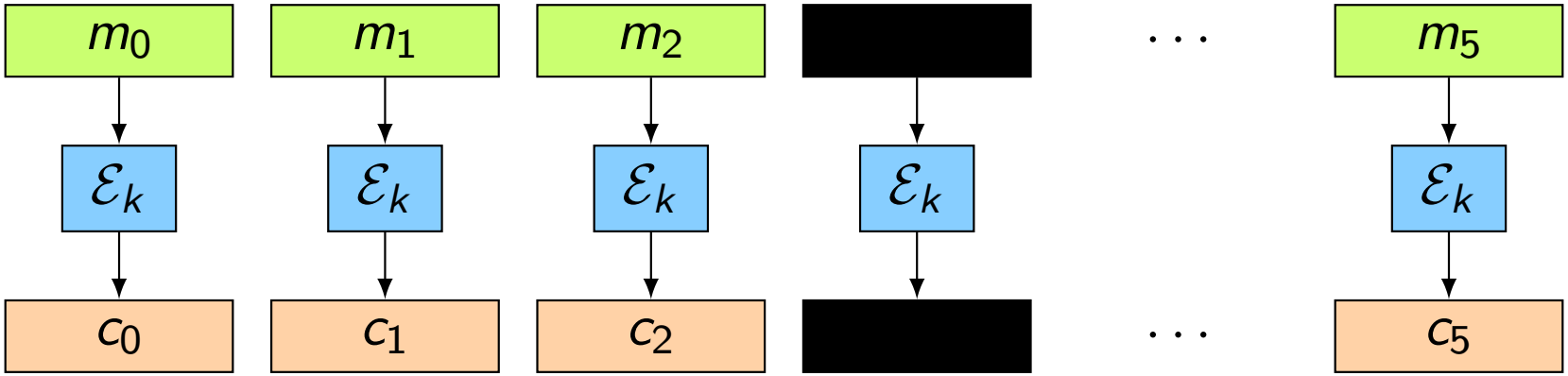


ECB: BLOCS INDÉPENDANTS



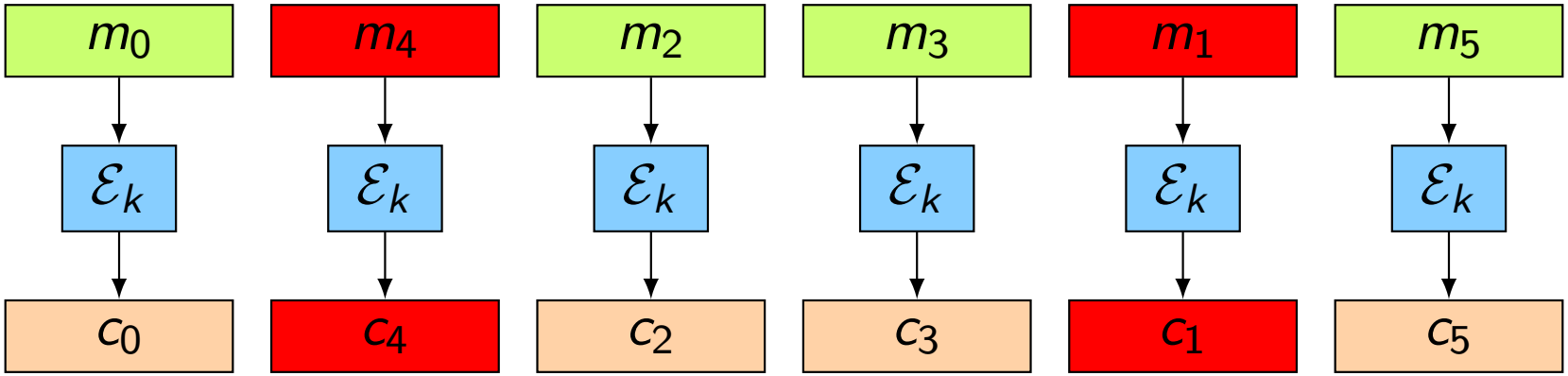


ECB: SUPPRESSION DE BLOCS



Suppression triviale d'un bloc

ECB: ÉCHANGE DE BLOCS



Échange de deux blocs

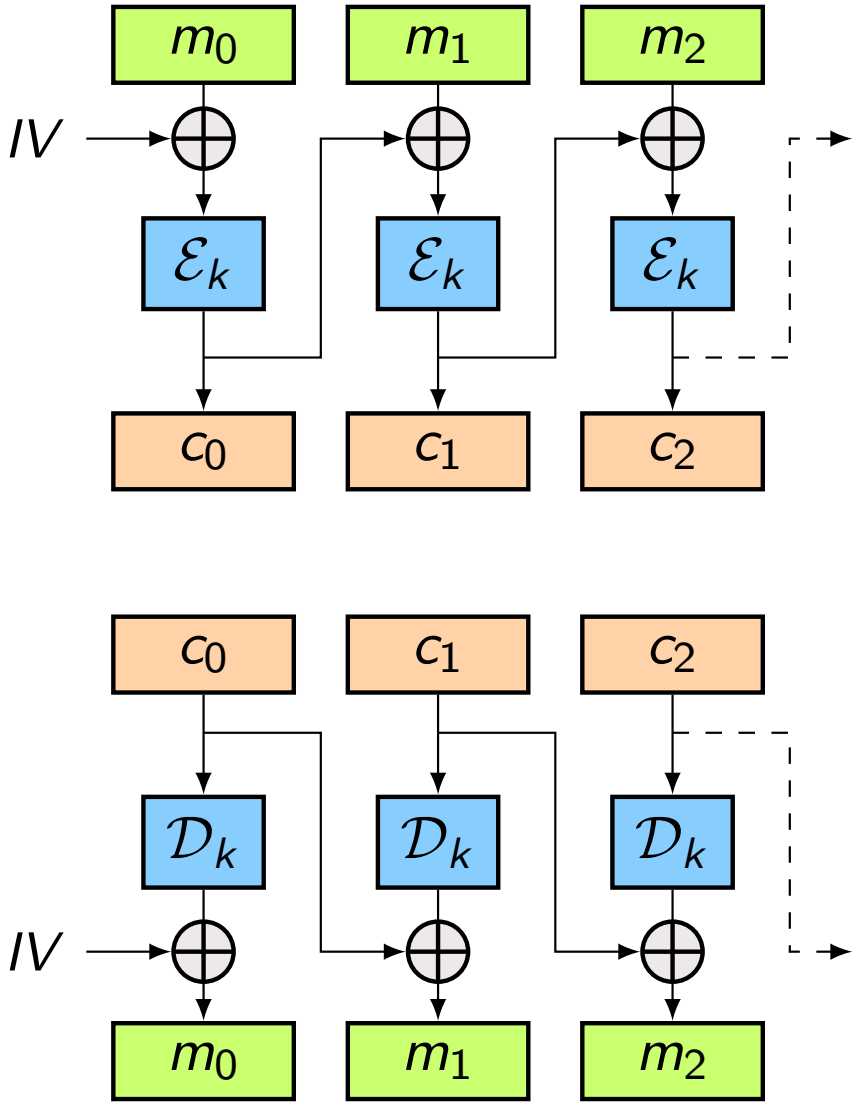
MODES OPÉRATOIRES: CBC

Mode CBC (*Cipher Block Chaining*)

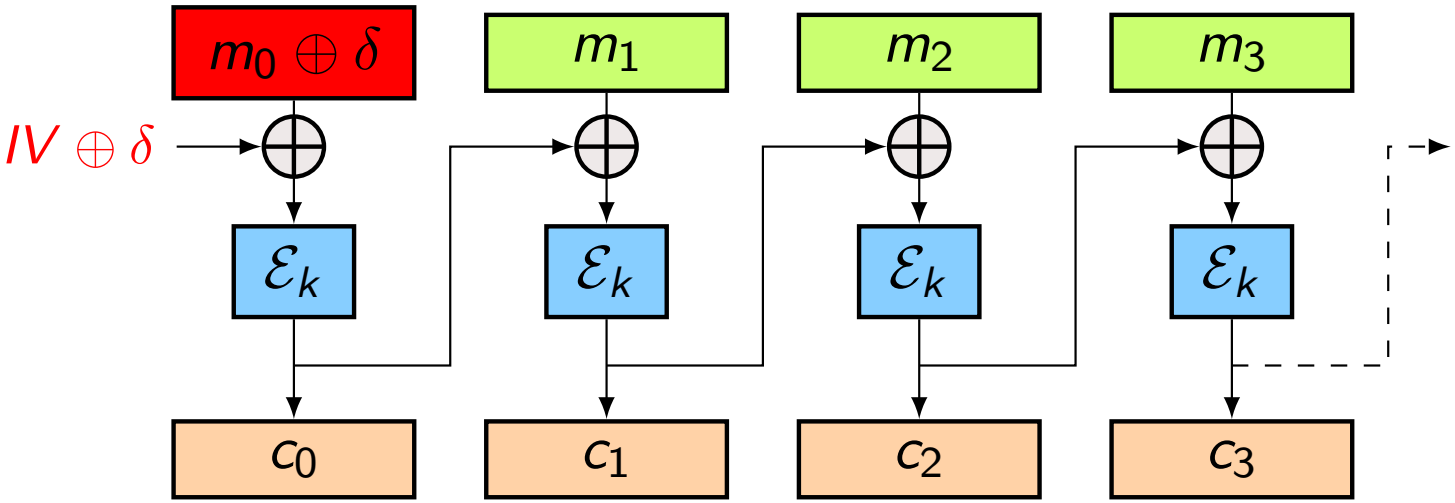
Le chiffré précédent est réinjecté dans les suivants

Un bloc dépend de tous les précédents

Mode randomisés par la présence d'une valeur aléatoire initiale (IV = *Initial Value*)

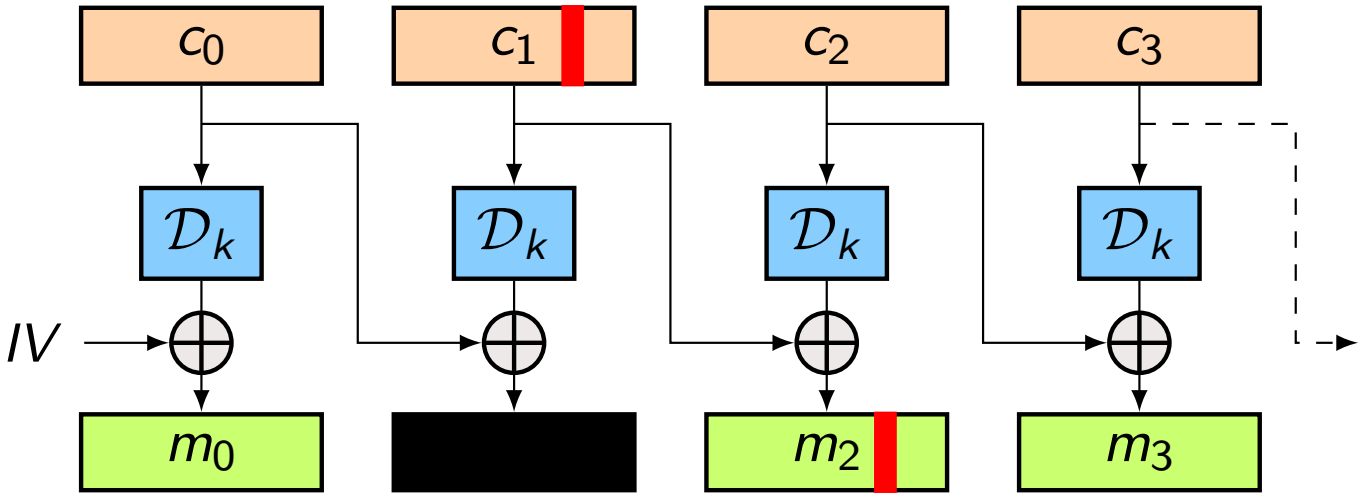


MODES OPÉRATOIRES: CBC



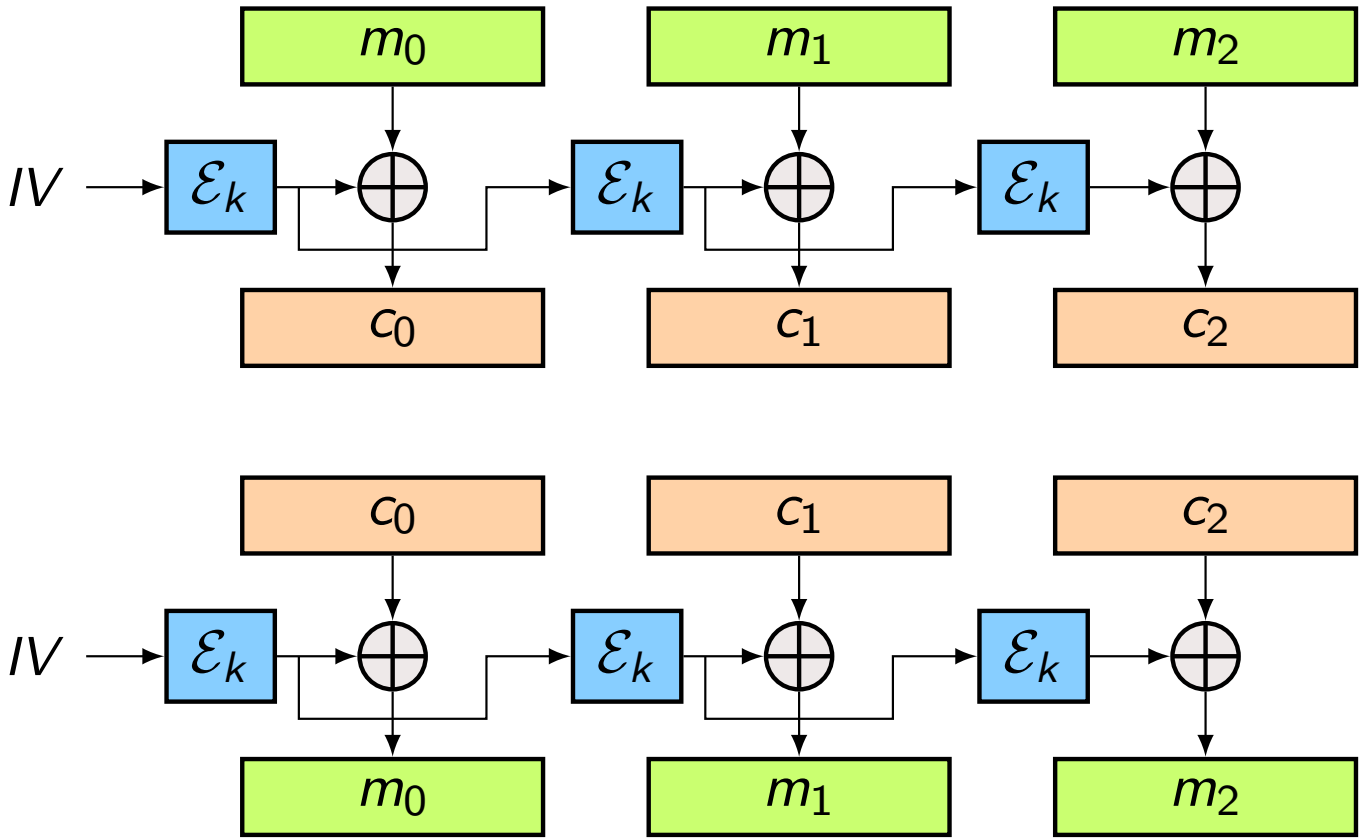
Modification arbitraire du premier bloc

MODES OPÉRATOIRES: CBC



MODES OPÉRATOIRES: OFB

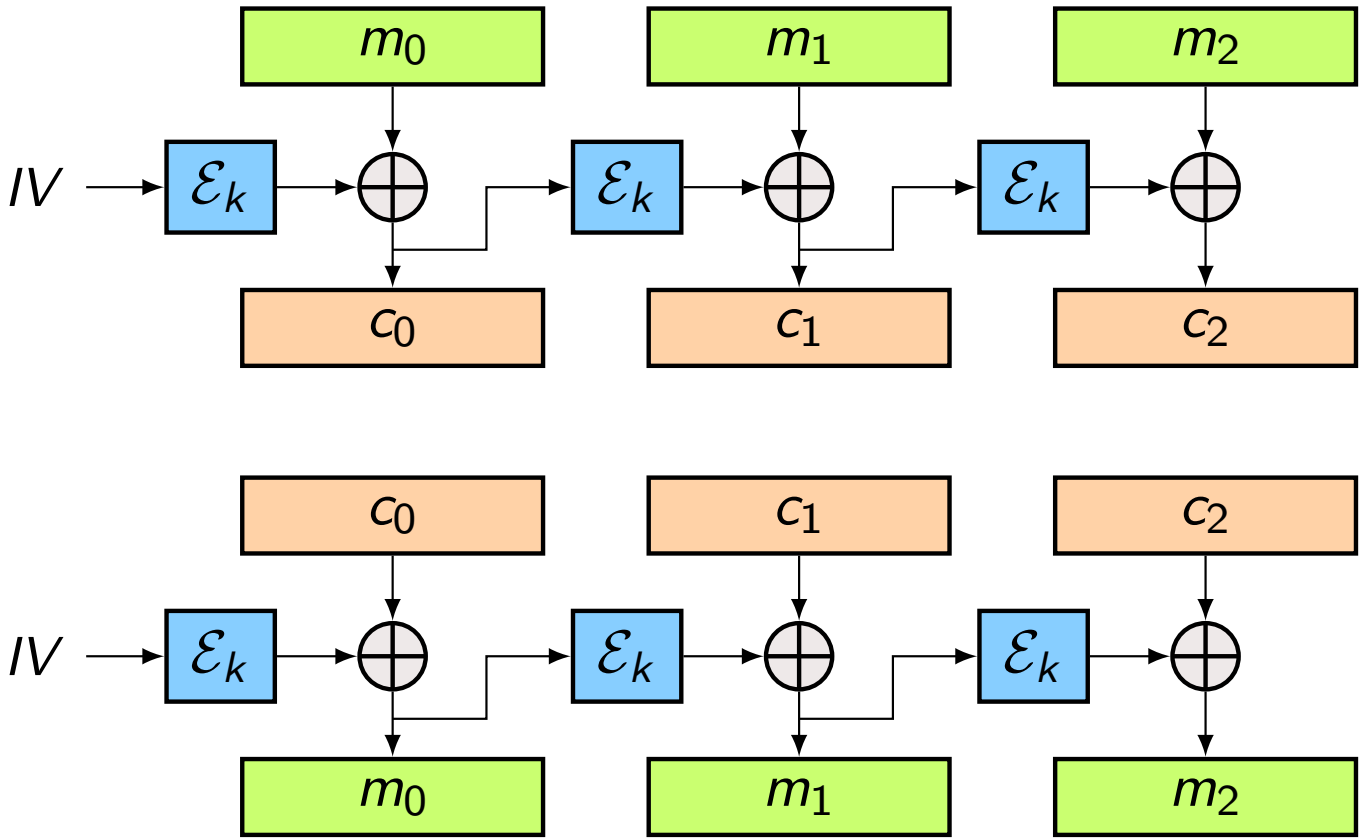
Le mode OFB (*Output FeedBack*)



Comportement similaire à un chiffrement par flot

MODES OPÉRATOIRES: CFB

Le mode CFB (*Cipher FeedBack*)



Comportement similaire à un chiffrement par flot

II. CHIFFREMENT ASYMÉTRIQUE

II.1. MODES OPÉRATOIRES

Organisation de la section « MODES OPÉRATOIRES »

PKCS#1 v1.5
PKCS#1 v2.1 (OAEP)
Chiffrement hybride

LES MODES OPÉRATOIRES DE CHIFFREMENT ASYMÉTRIQUES

Comment atteindre la sécurité IND-CCA avec des chiffrements qui sont multiplicatifs (RSA) ?

Plusieurs solutions (à combiner entre elles):

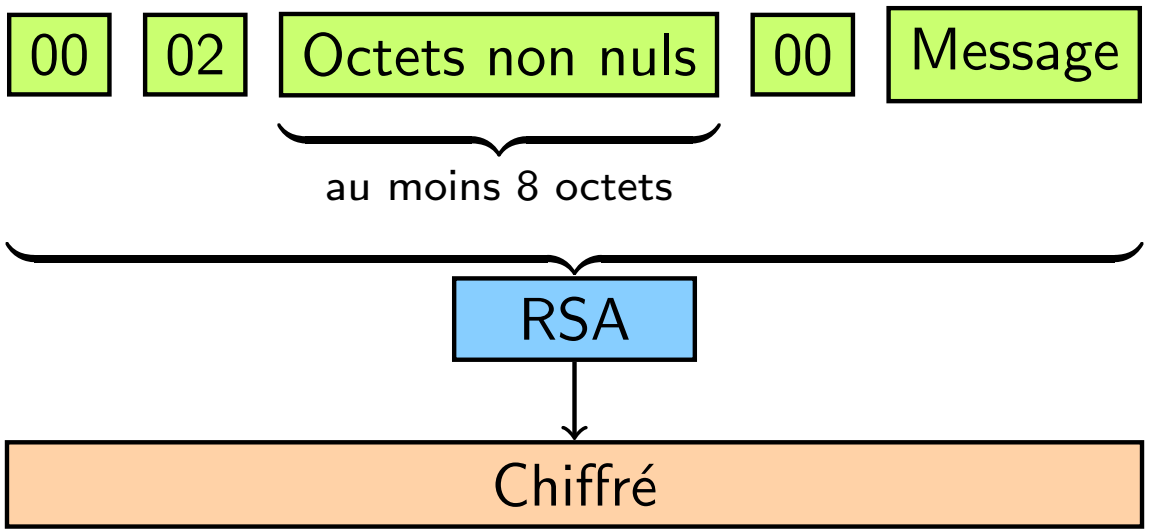
1. imposer un formatage (*padding*,. . .)
2. briser la multiplicativité (hachage)
3. empêcher la malléabilité (fonction à sens unique)
4. . . .

Des transformations génériques existent

LA NORME PKCS#1 V1.5 EN CHIFFREMENT

Public-Key Cryptography Standard

- Norme publiée par RSA Security Inc.



RSA PKCS#1 V1.5

Encapsulation prévue pour RSA, mais aucune preuve de sécurité

En particulier, pas de sécurité CCA:

- Un attaquant qui a accès à un oracle de validation de chiffré peut déchiffrer un message
- Mise en œuvre dans SSL3: le serveur renvoie une erreur quand le message déchiffré n'est pas conforme à PKCS#1

ATTAQUE SUR PKCS#1 V1.5

Attaque à chiffrés choisis proposée par Bleichenbacher à Crypto 98

Principe: *accès à un oracle de validité*

- oracle qui prend un chiffré en entrée et répond 1 ou 0 suivant que le clair sous-jacent est correctement formaté

Par un certain nombre de requêtes à cet oracle, l'attaquant peut déchiffrer un message chiffré

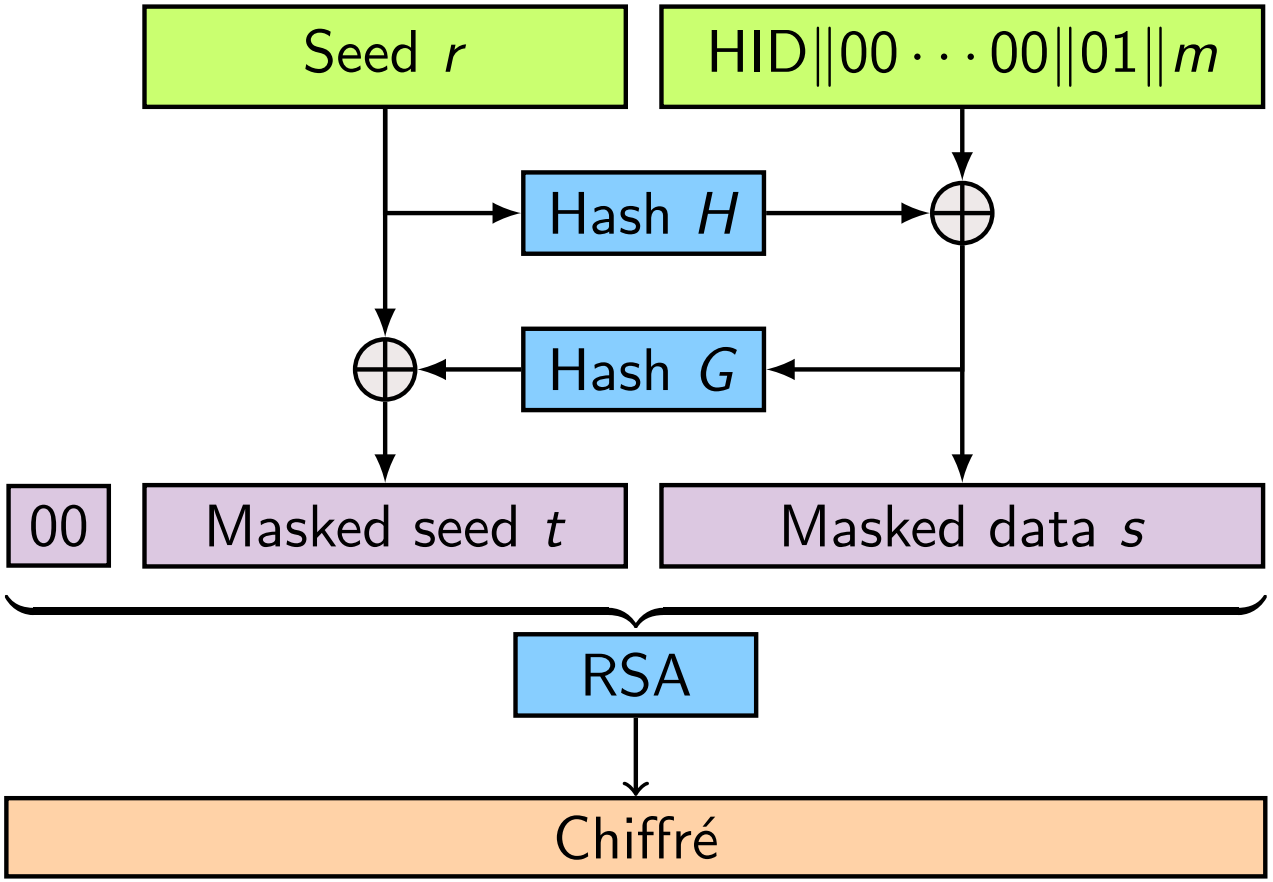
ATTAQUE SUR PKCS#1 V1.5

Détails de l'attaque

1. L'attaquant doit déchiffrer un challenge C
2. Il génère des chiffrés $C_1, C_2, \ldots$ liés à C par: $C_i = C \cdot r_i^e \bmod n$, où r_i est un aléa et (n, e) la clé publique
3. Il interroge l'oracle qui répond si le clair sous-jacent (i.e., $M \cdot r_i$) est correct ou non
4. Un $M \cdot r_i$ valide permet d'obtenir un encadrement de M
5. Le choix des r_i est adaptatif (CCA2): on réutilise les encadrements obtenus pour choisir les r_i à venir
6. L'attaquant apprend petit à petit des bits d'information sur M
7. Pour un module de 1024 bits, il faut $\approx$ un million de requêtes

PKCS#1 V2.1: RSA-OAEP
Optimal Asymmetric Encryption Padding

- Proposé en 1994 par Bellare et Rogaway



OAEP: REBONDISSEMENTS

PKCS#1 v2.1 = RSA-OAEP a eu très chaud...

1994: Bellare et Rogaway proposent OAEP

2000: Shoup exhibe une erreur dans la preuve

 erreur *intrinsèque* et non-réparable !

2000: Pointcheval prouve que cette erreur est réparable pour RSA

2001: RSA-OAEP est prouvé sûr et le critère nécessaire pour OAEP est exhibé (*partial-domain one-way permutation*)

2001: Alternatives à OAEP: OAEP+, SAEP,...

RSA-OAEP: SÉCURITÉ

RSA-OAEP est prouvé sûr, mais inefficace...

- Il y a une preuve de sécurité mais la réduction au problème RSA est de mauvaise qualité:

$$\mathrm{Adv}_{OAEP}(t) \leq \sqrt{4\mathrm{Adv}_{RSA}(2^t)}$$

- Pour une sécurité en 2^{-80} il faut donc $\mathrm{Adv}_{RSA}(2^t) \leq 2^{-160}$
- La taille du modulo qui en résulte est (au moins) de 4096 bits...

CHIFFREMENT MIXTE

Combiner les avantages de la clé publique et de la clé secrète

1. Le chiffrement asymétrique est pratique (clé publique) mais lent. . .
   - tailles de clés importantes
   - opérations mathématiques sophistiquées
2. Le chiffrement symétrique est performant
   - opérations de bas niveau sur les bits
   - facilement implantable sur matériel

   mais nécessite une clé commune secrète

PRINCIPE DU CHIFFREMENT MIXTE

Chiffrement mixte (ou hybride)

- On chiffre avec une clé publique une clé de session (symétrique) aléatoire
- Cette clé de session sera utilisée pour chiffrer et/ou authentifier les messages

Question: qui choisit la clé ?
Échange de clé, ou distribution de clé