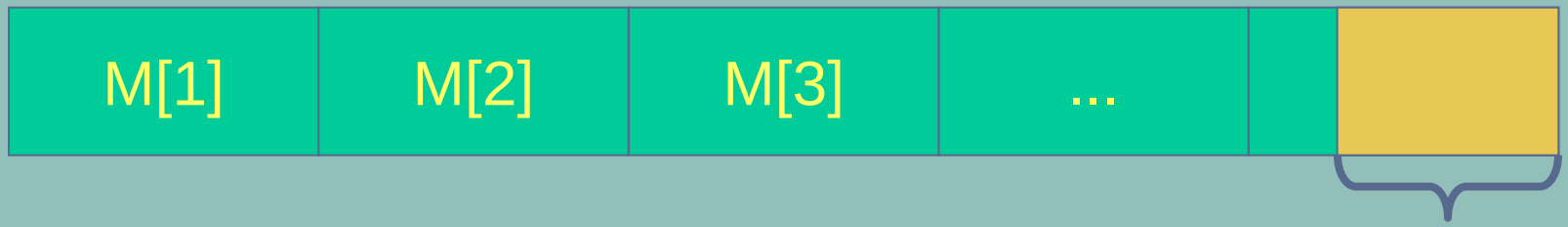
Les modes opératoires de la cryptographie symétrique

Jang Schiltz
Enseignant-chercheur au Centre Universitaire de Luxembourg

Rembourrage

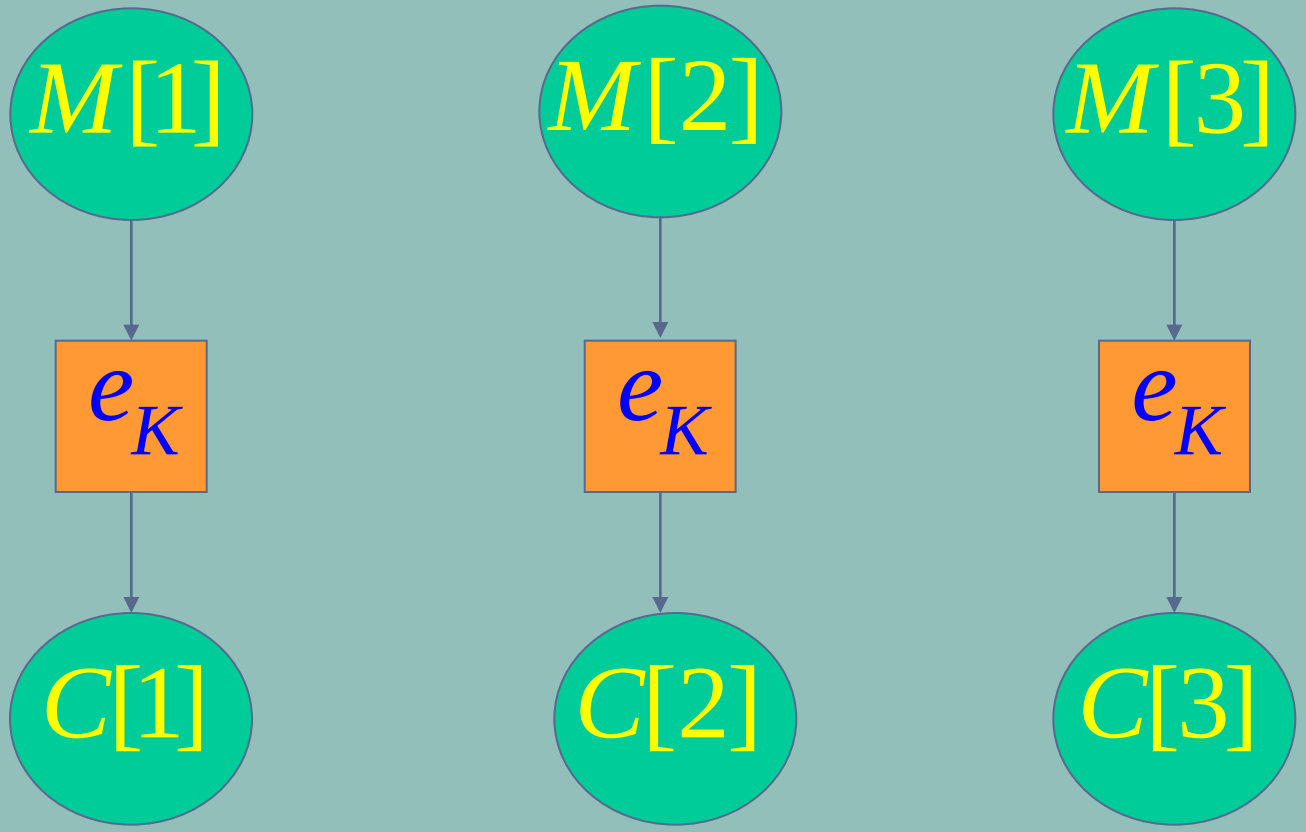
Que faire quand la longueur d'un message n'est pas égal à un multiple de la longueur d'un bloc?



Il manque n mots

M[1]	M[2]	M[3]	...		nnn...n
M[1]	M[2]	M[3]	...		123...n
M[1]	M[2]	M[3]	...		000...n
M[1]	M[2]	M[3]	...		$r_1 r_2 r_3 ... n$

Le mode ECB (Chiffrement)

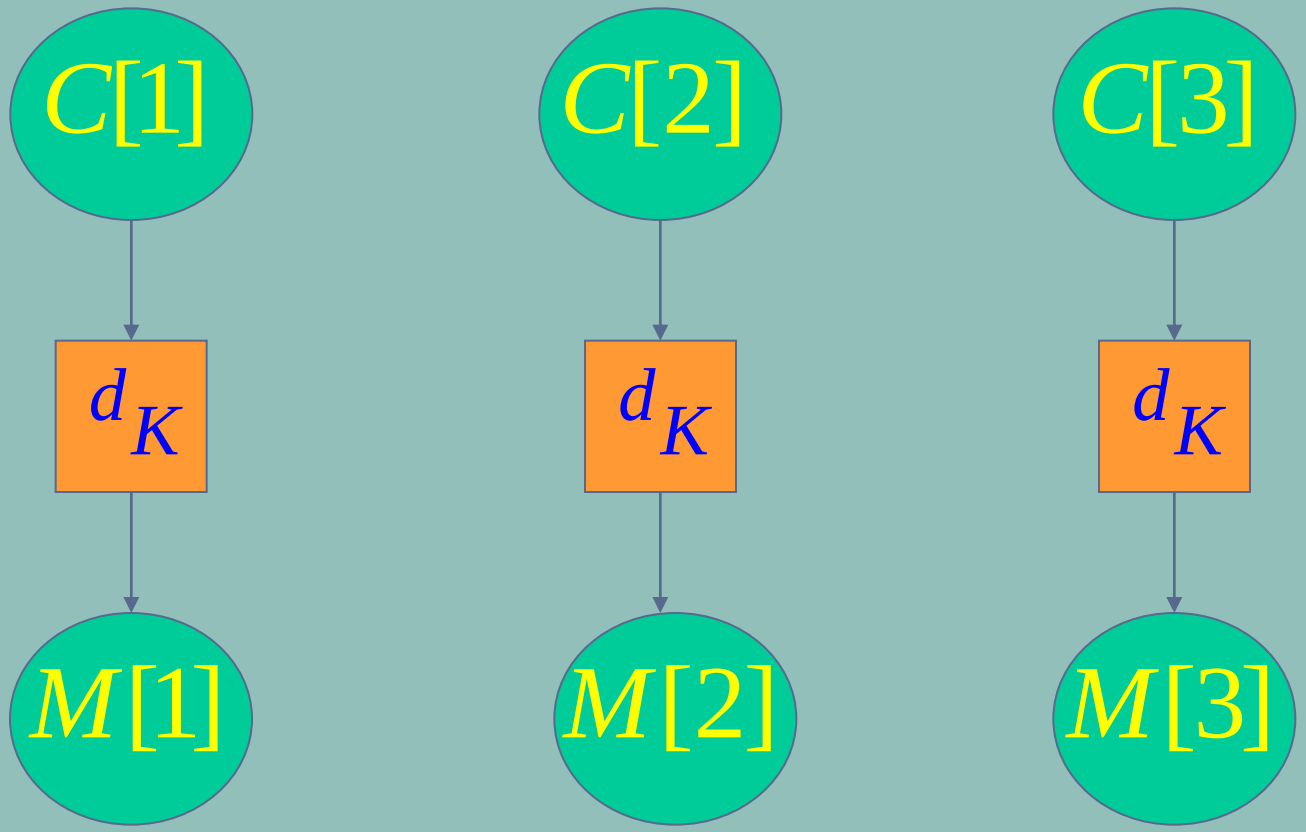


$$C[n] = e\left(M[n]\right), \text{ pour n} = 1,\ldots,N$$

Cryptology & Security Initiative

Centre Universitaire de Luxembourg
CRP Gabriel Lippmann

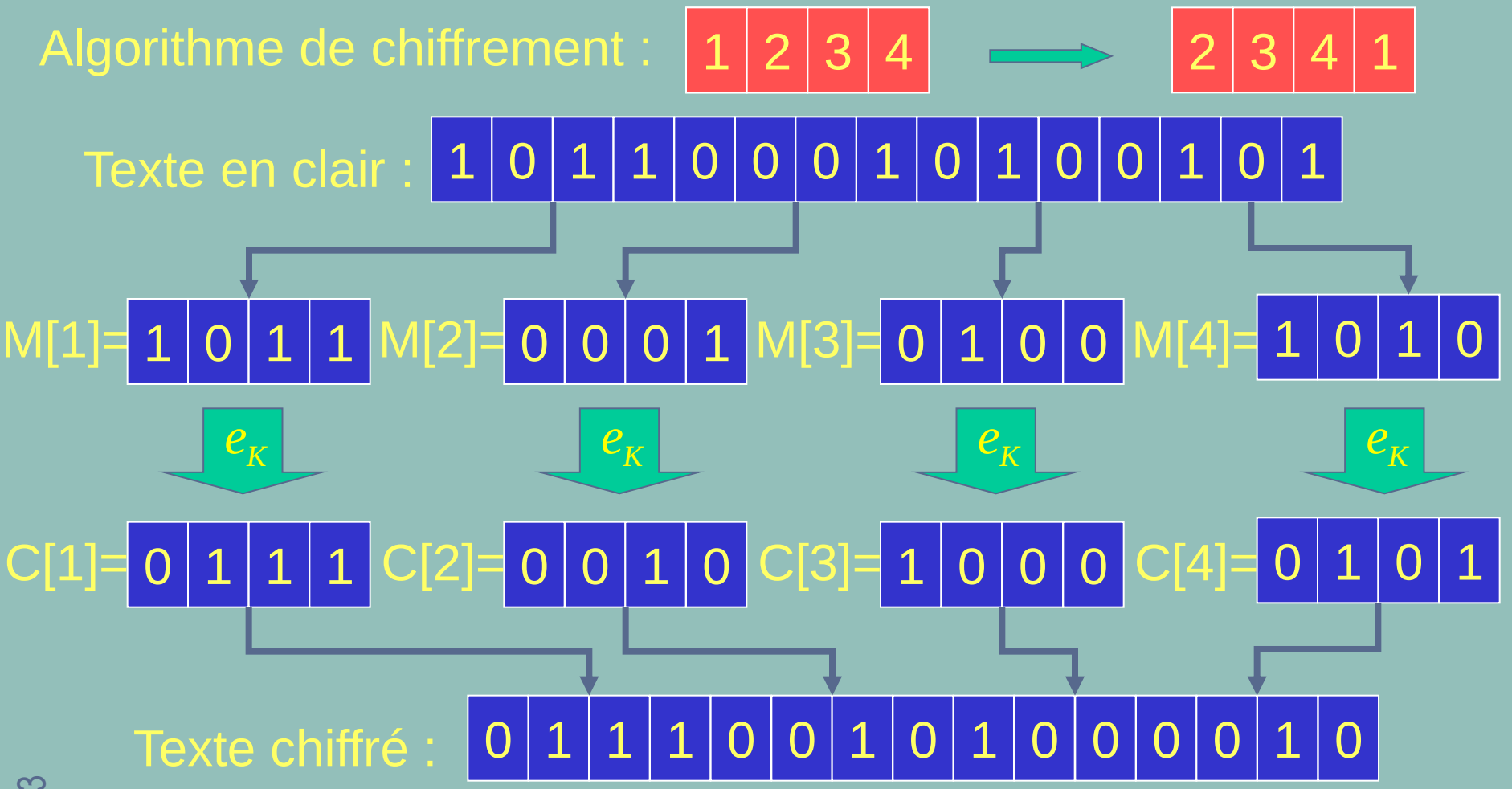
Le mode ECB (Déchiffrement)



$$M[n] = d\left(C[n]\right), \text{ pour n} = 1,\ldots,N$$

Cryptology & Security Initiative
Centre Universitaire de Luxembourg
CRP Gabriel Lippmann

Exemple en mode ECB



Avantages du mode ECB

Méthode rapide et facile à implémenter

Chiffrement de chaque bloc indépendant des autres

Utilisation pour des bases de données

Désavantages du mode ECB (1)

Cryptology & Security Initiative

Textes en clair identiques
⇒Textes chiffrés identiques

Possibilité de construire des carnets de codage

Les messages ont souvent un début ou une fin standardisés!!

Désavantages du mode ECB (2)

Utilisé uniquement pour des messages aléatoires courts, comme des clés cryptographiques !!!

Messages de transfert d'argent standards :

M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13
date	Banques émettrice et bénéficiaires			Nom du déposant					Numéro de compte			Montant

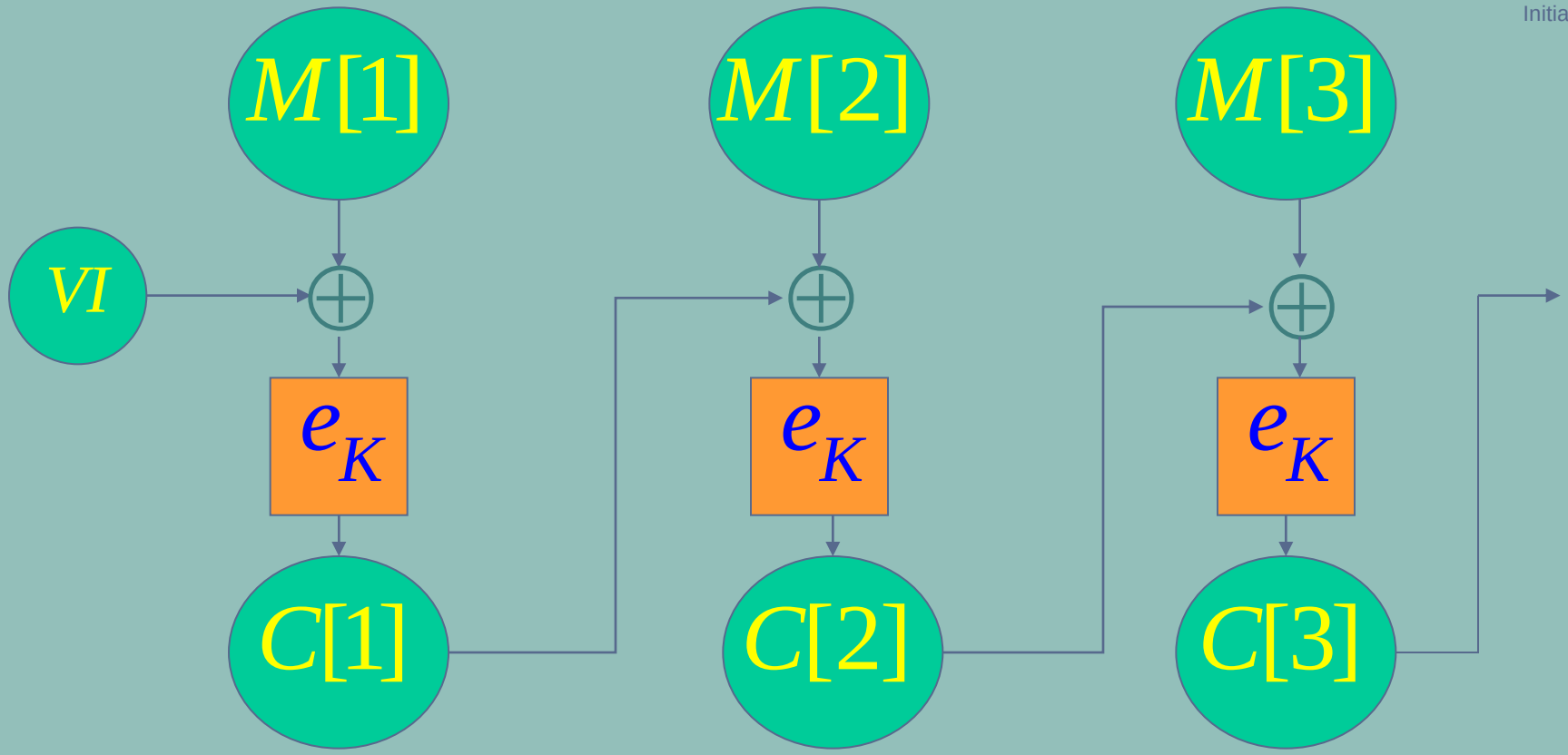
Propagation d'erreurs

Cryptology & Security Initiative

Erreur d'un bit dans un bloc ⇒ Ce bloc est mal déchiffré mais Pas d'influence sur d'autres blocs

Erreur de synchronisation ⇒ Tout est embrouillé et Rétablissement au premier bloc complètemennt resynchronisé

Le mode CBC (Chiffrement)

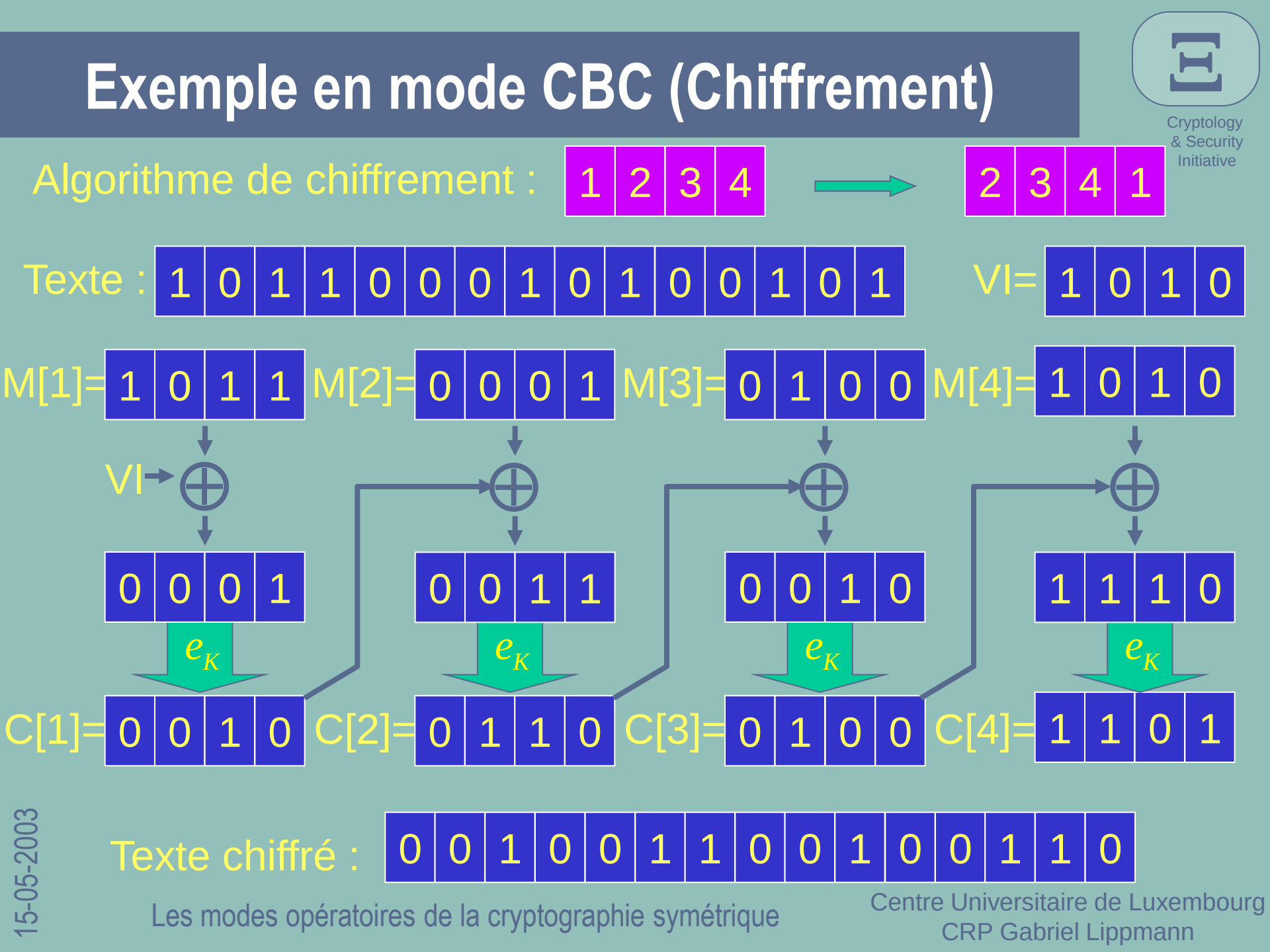


$$C[1] = e\left(M[1] \oplus VI\right)$$

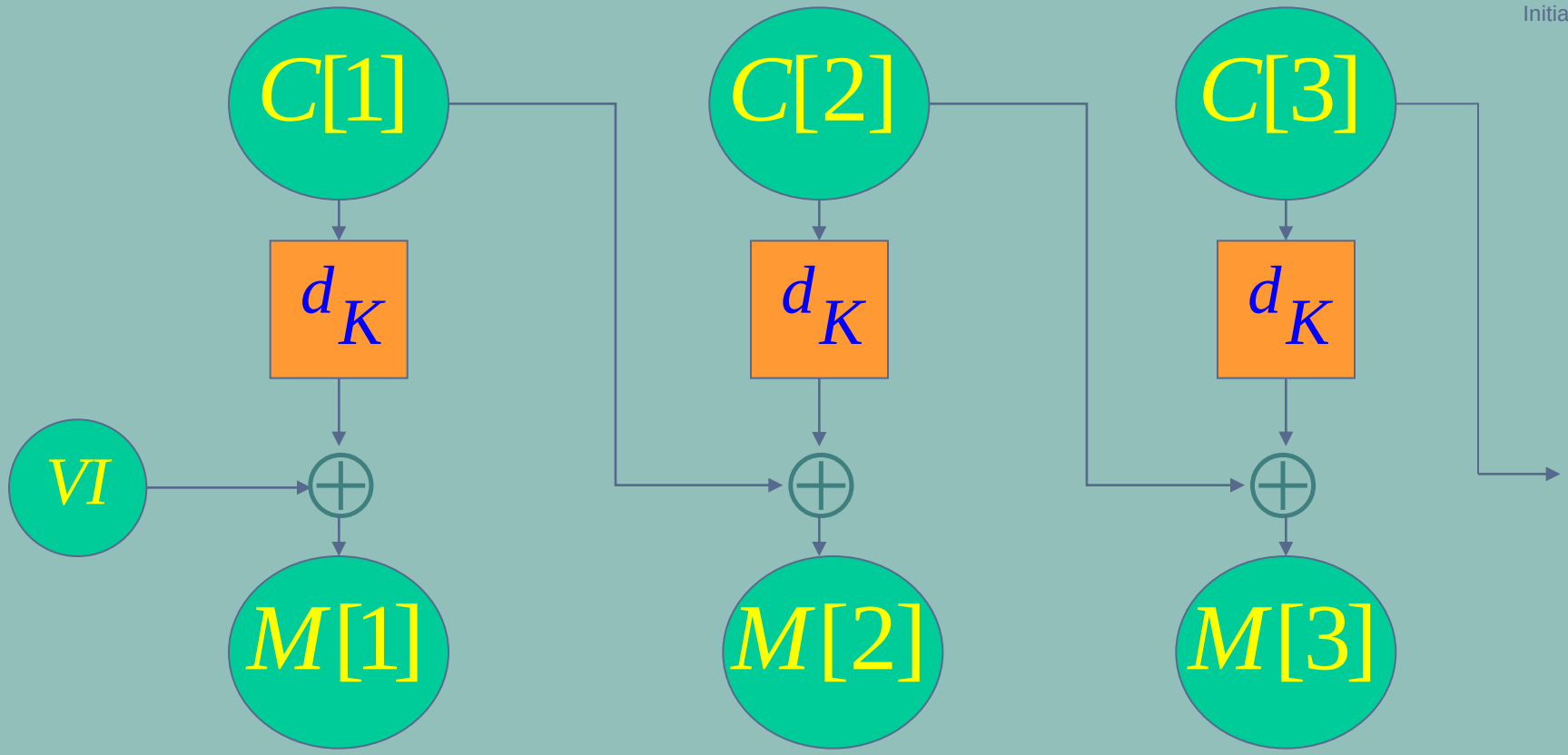
$$C[n] = e\left(M[n] \oplus C[n-1]\right), \text{ pour } n = 2,\ldots,N$$

Centre Universitaire de Luxembourg
CRP Gabriel Lippmann

Exemple en mode CBC (Chiffrement)



Le mode CBC (Déchiffrement)



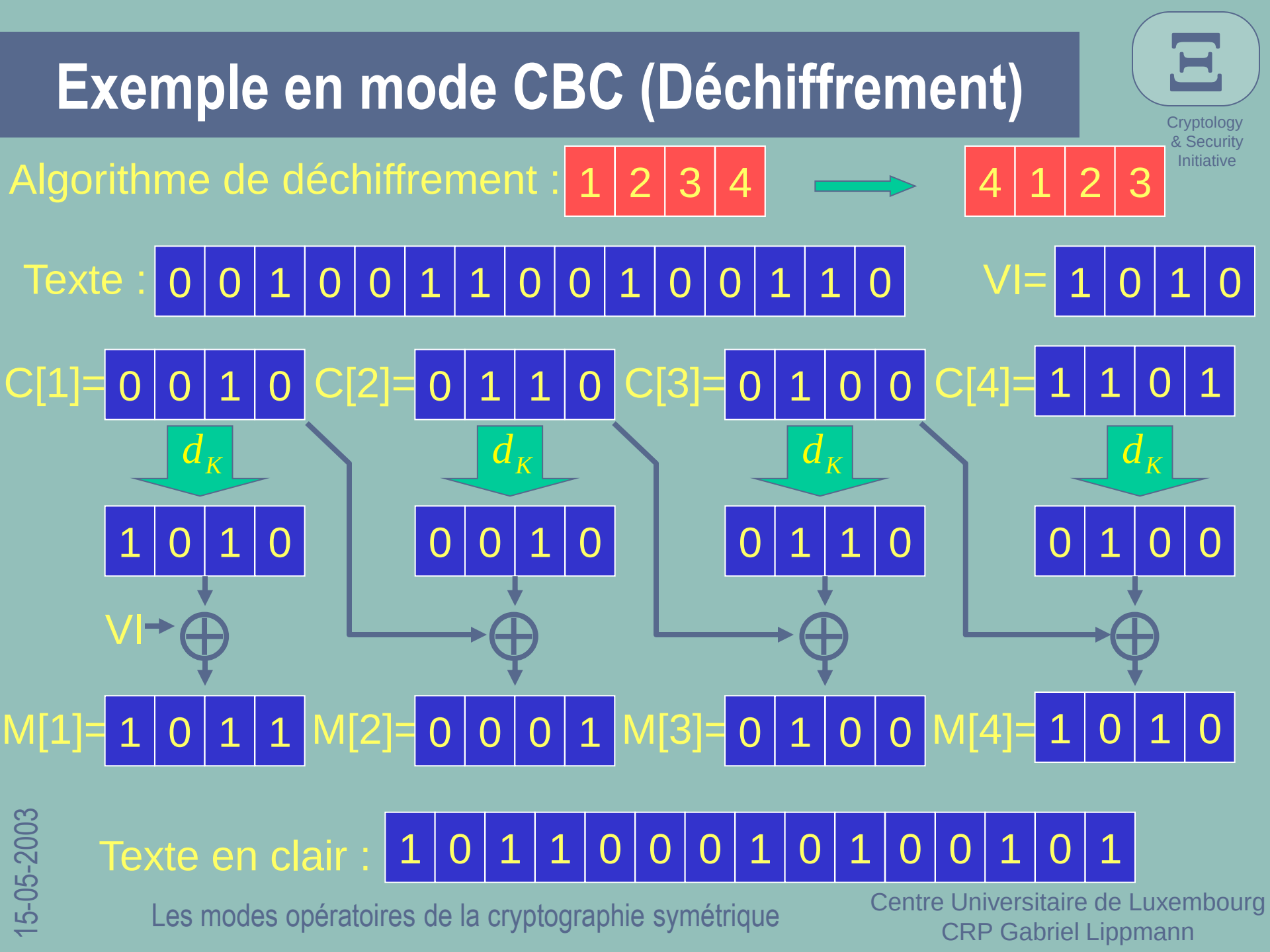
$$M[1] = d\left(C[1]\right) \oplus VI$$

$$M[n] = d\left(C[n]\right) \oplus C[n\text{-}1], \text{ pour } n = 2,\ldots,N$$

Cryptology & Security Initiative

Centre Universitaire de Luxembourg
CRP Gabriel Lippmann

Exemple en mode CBC (Déchiffrement)



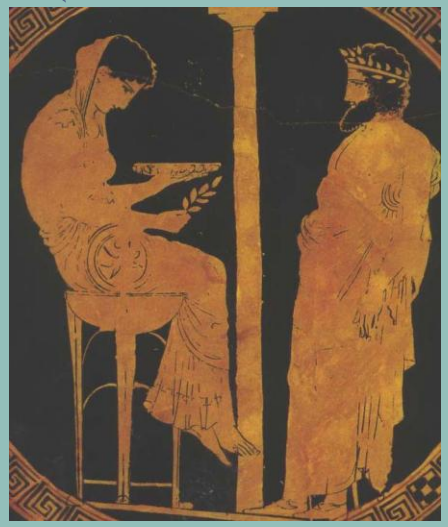
Oracle de contrôle de rembourrage

Cryptology & Security Initiative

Le rembourrage est incorrect

Le rembourrage est correct

C

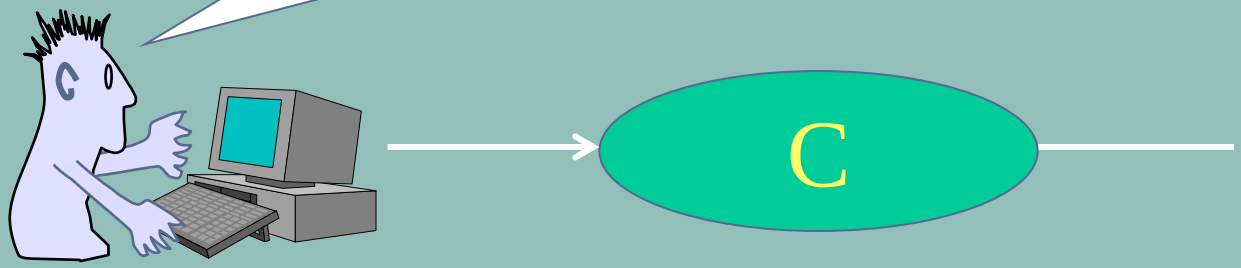


déchiffrement et vérification rembourrage

Attaque de Vaudenay (Oracle qui explose)

Cryptology & Security Initiative

Est-ce que $W_1 \ldots W_m$ est une bonne fin de $d(C)$?



Attaque de Vaudenay

M

serveur

$C = e_K(M)$

C|W

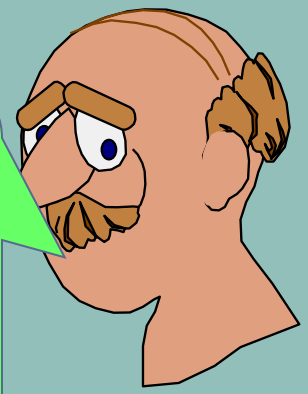
OK / KO

Propriétés du mode CBC

Cryptology & Security Initiative

Méthode rapide et facile à implémenter

Changer à chaque fois le vecteur d'initialisation !



Méthode très souvent utilisé!

Méthode sûre si on fait attention au rembourrage

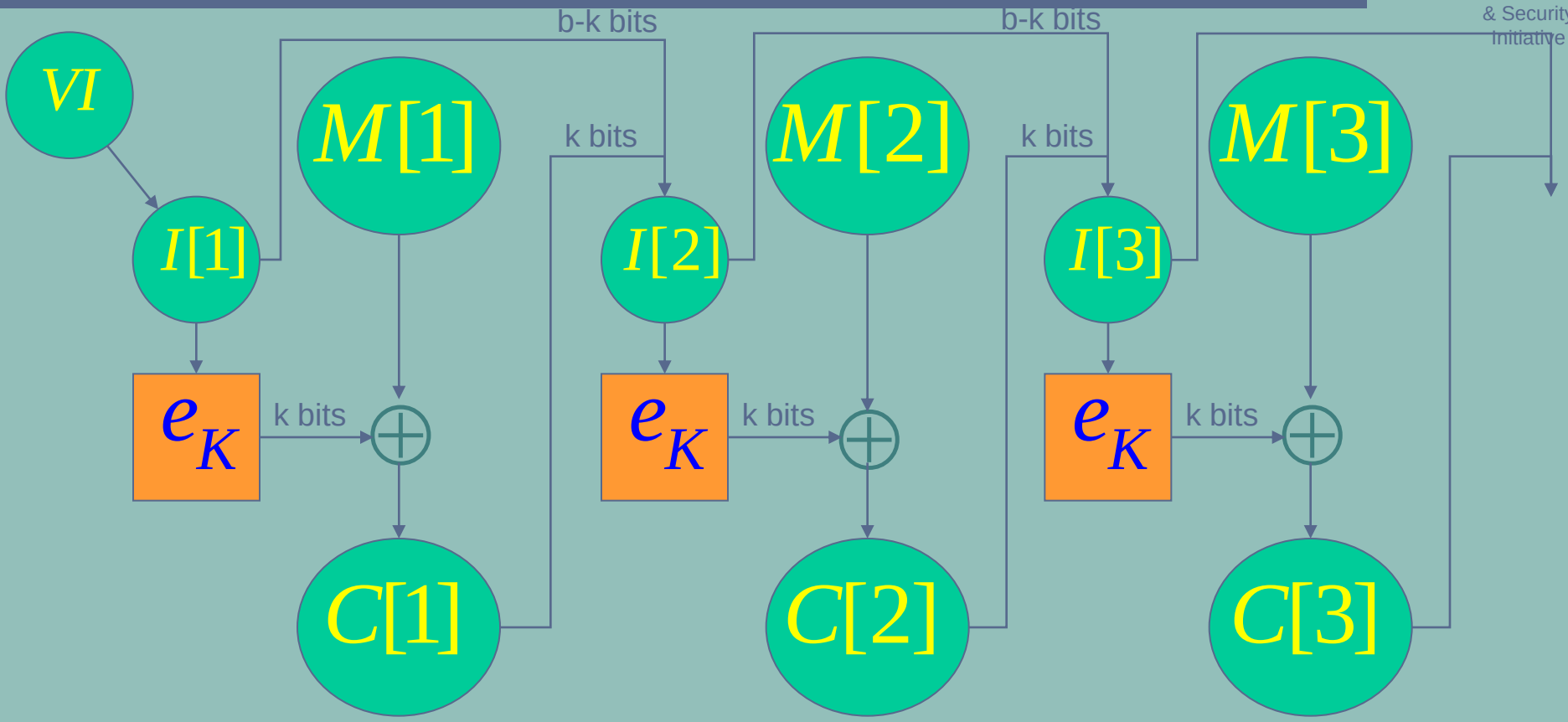
Blocs de texte chiffré dépendent de tous les blocs de texte en clair précédents

Propagation d'erreurs

Erreur d'un bit dans un bloc $\Rightarrow$ Ce bloc est mal déchiffré et Erreur d'un bit dans le bloc qui suit

Erreur de synchronisation $\Rightarrow$ Tout est embrouillé et Rétablissement au premier bloc complètemennt resynchronisé

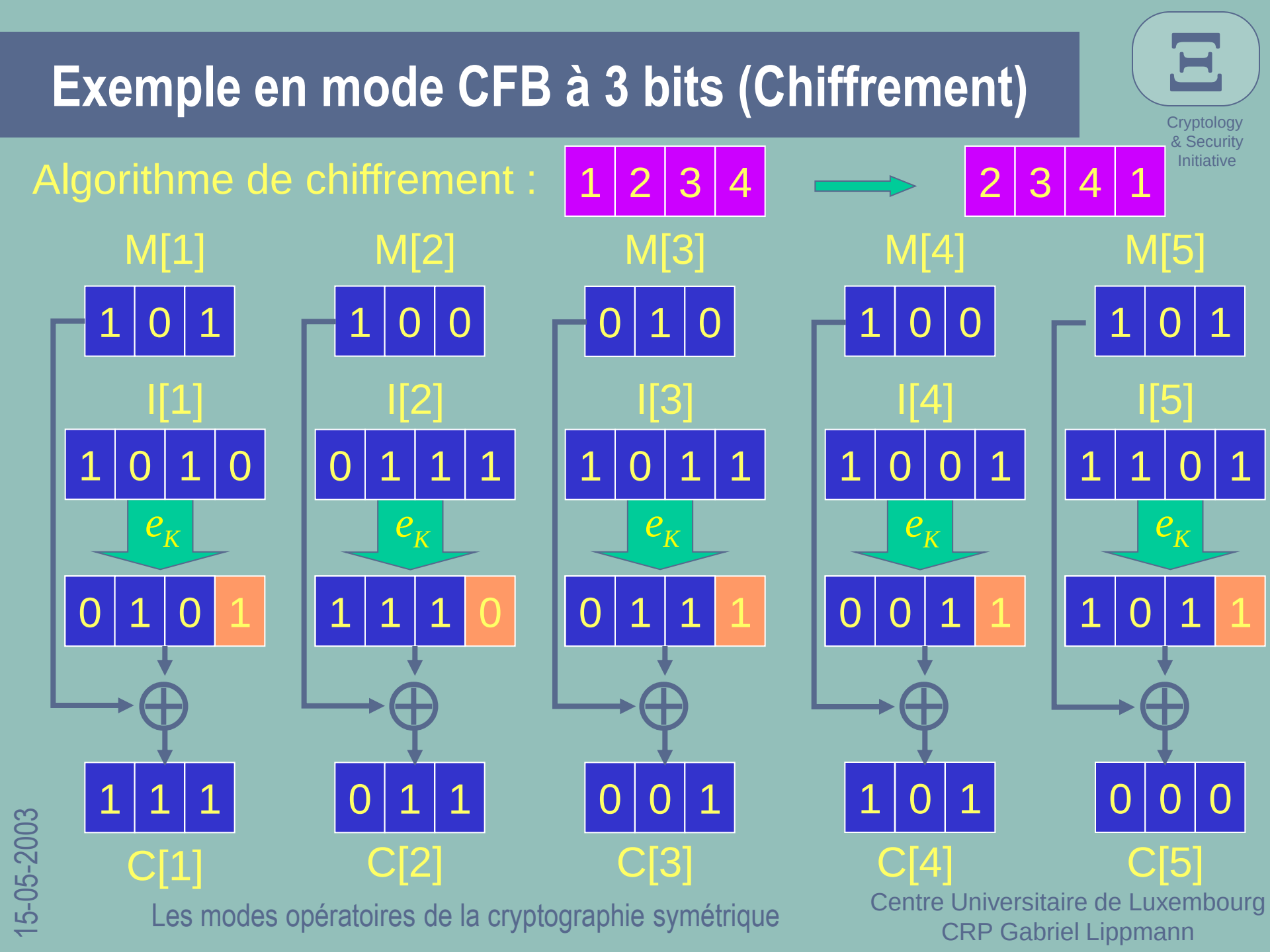
Le mode CFB (Chiffrement)



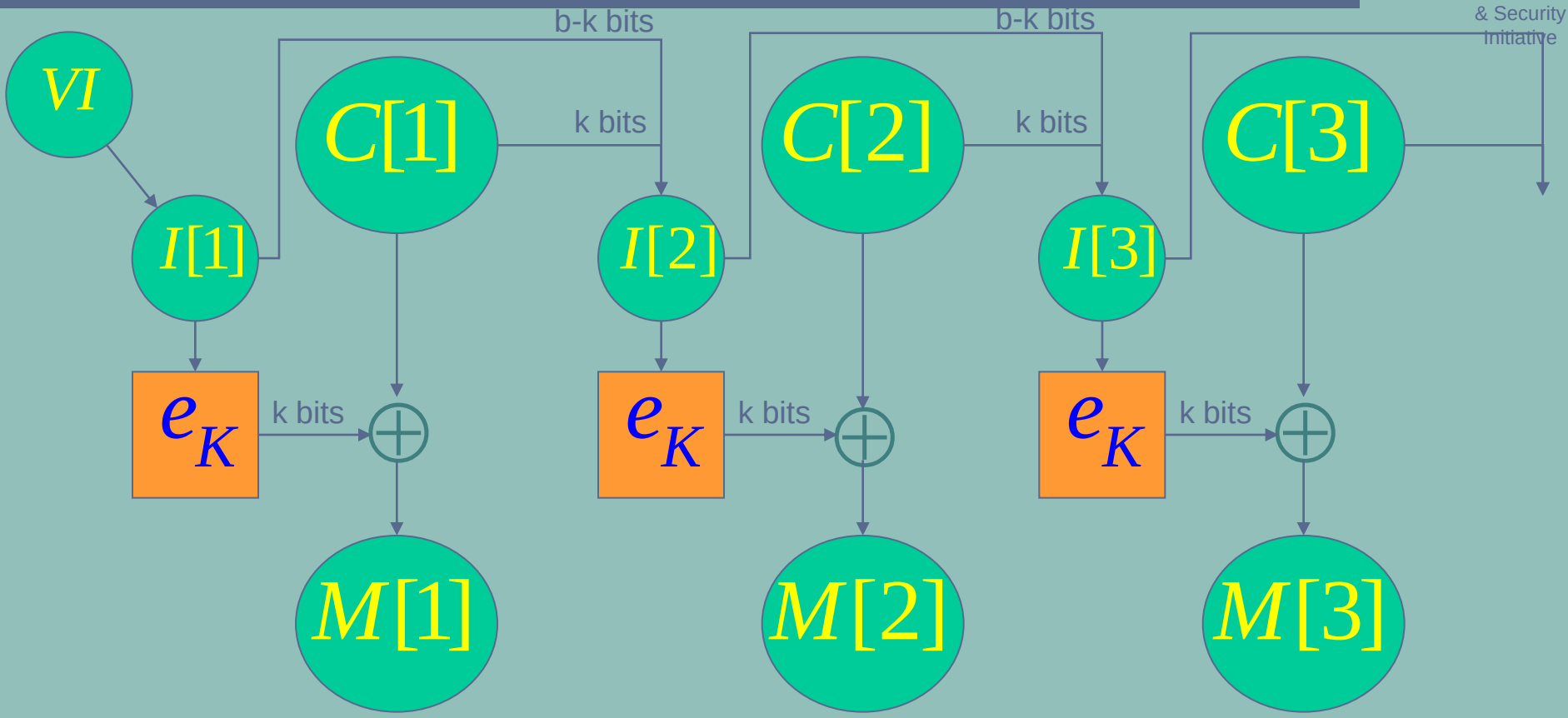
$$I[1]=VI$$
$$I[n]=\left(I[n-1]<<k\right)|C[n-1],\ \text{pour n}=2,\ldots,N$$
$$C[n]=M[n]\oplus MSB_k\left(e(I[n])\right),\ \text{pour n}=1,\ldots,N$$

Centre Universitaire de Luxembourg
CRP Gabriel Lippmann

Exemple en mode CFB à 3 bits (Chiffrement)



Le mode CFB (Déchiffrement)



$$I[1]=VI$$

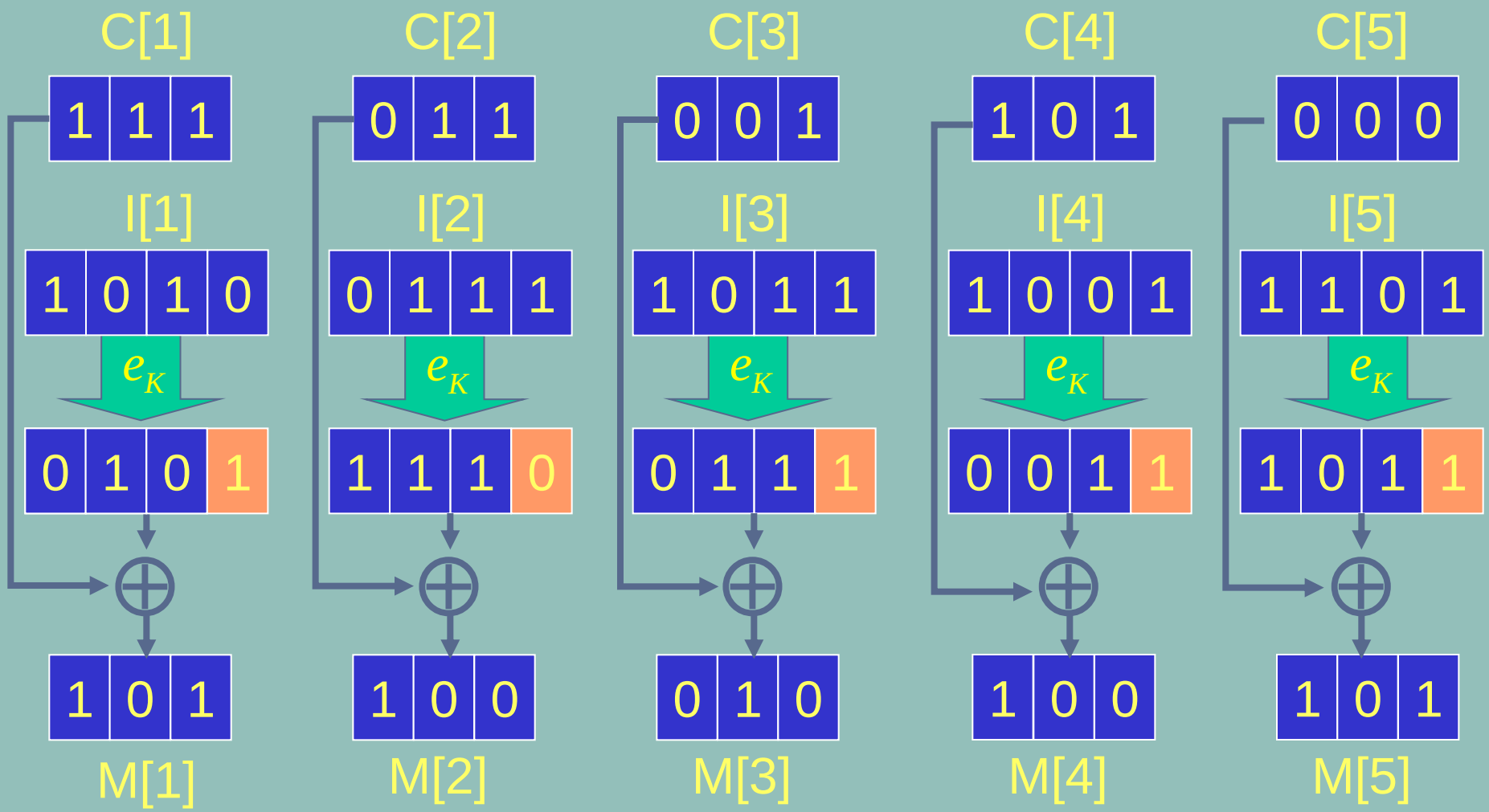
$$I[n]=\left(I[n-1]<<k\right)|C[n-1],\ \text{pour n}=2,\ldots,N$$

$$M[n]=C[n]\oplus MSB_k\left(e(I[n])\right),\ \text{pour n}=1,\ldots,N$$

Exemple en mode CFB à 3 bits (Déchiffrement)

Cryptology & Security Initiative

Algorithme de déchiffrement : 1 2 3 4 → 4 1 2 3



Propagation d'erreurs

Cryptology & Security Initiative

Erreur d'un bit dans un bloc ⇒ Tout est embrouillé jusqu'à la sortie de l'erreur du régistre à décalage

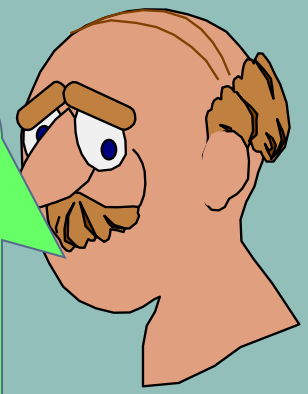
Erreur de synchronisation ⇒ Tout est embrouillé et Rétablissement dès la sortie de l'erreur du registre à décalage

Pas de problème de synchronisation, si k=1 !!

Propriétés du mode CFB

Méthode plus lente

Changer à chaque fois le vecteur d'initialisation !



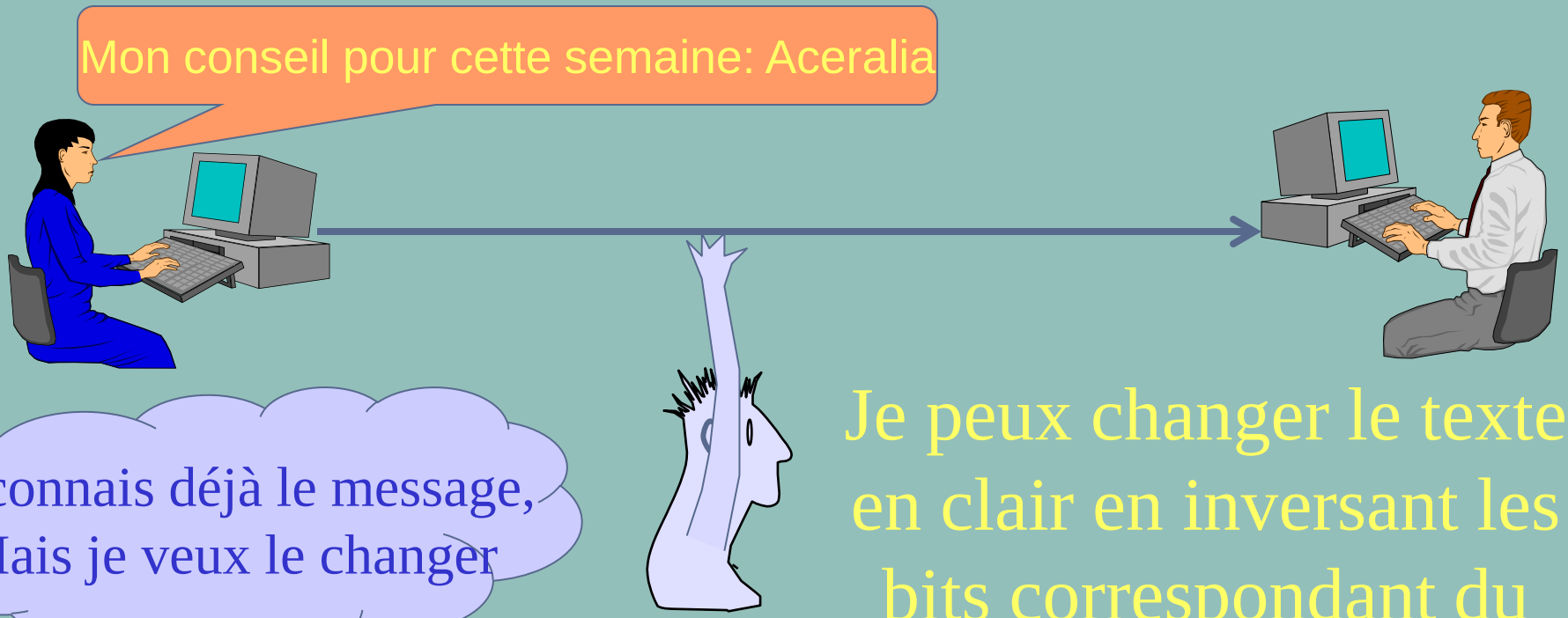
Méthode souvent utilisé pour chiffrer des données en continue

Même le déchiffrement utilise uniquement l'algorithme de chiffrement

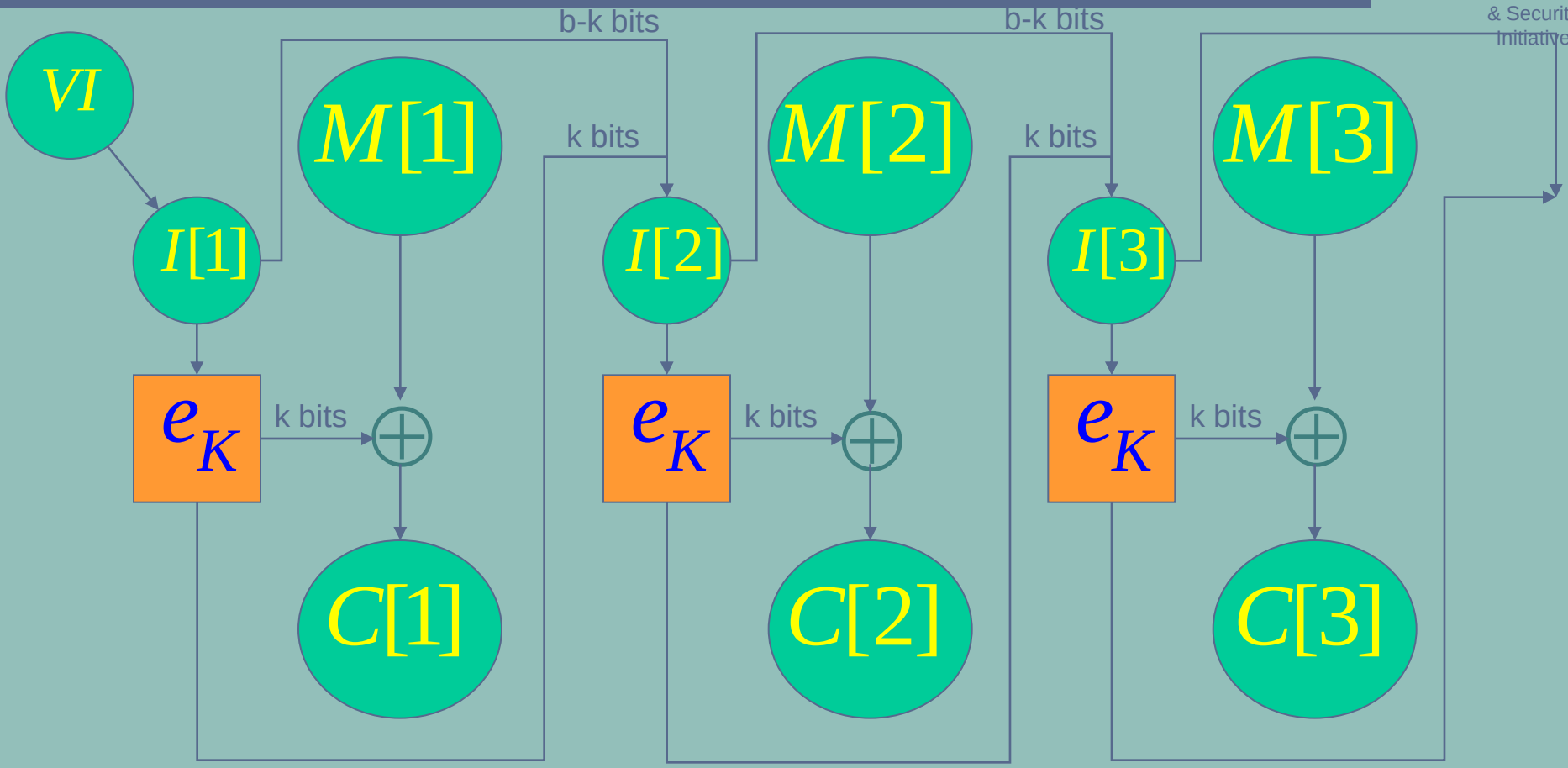
Blocs de texte chiffré dépendent de tous les blocs de texte en clair précédents

Bit flipping attack

Cryptology
& Security
Initiative



Le mode OFB (Chiffrement)



$$I[1] = VI$$

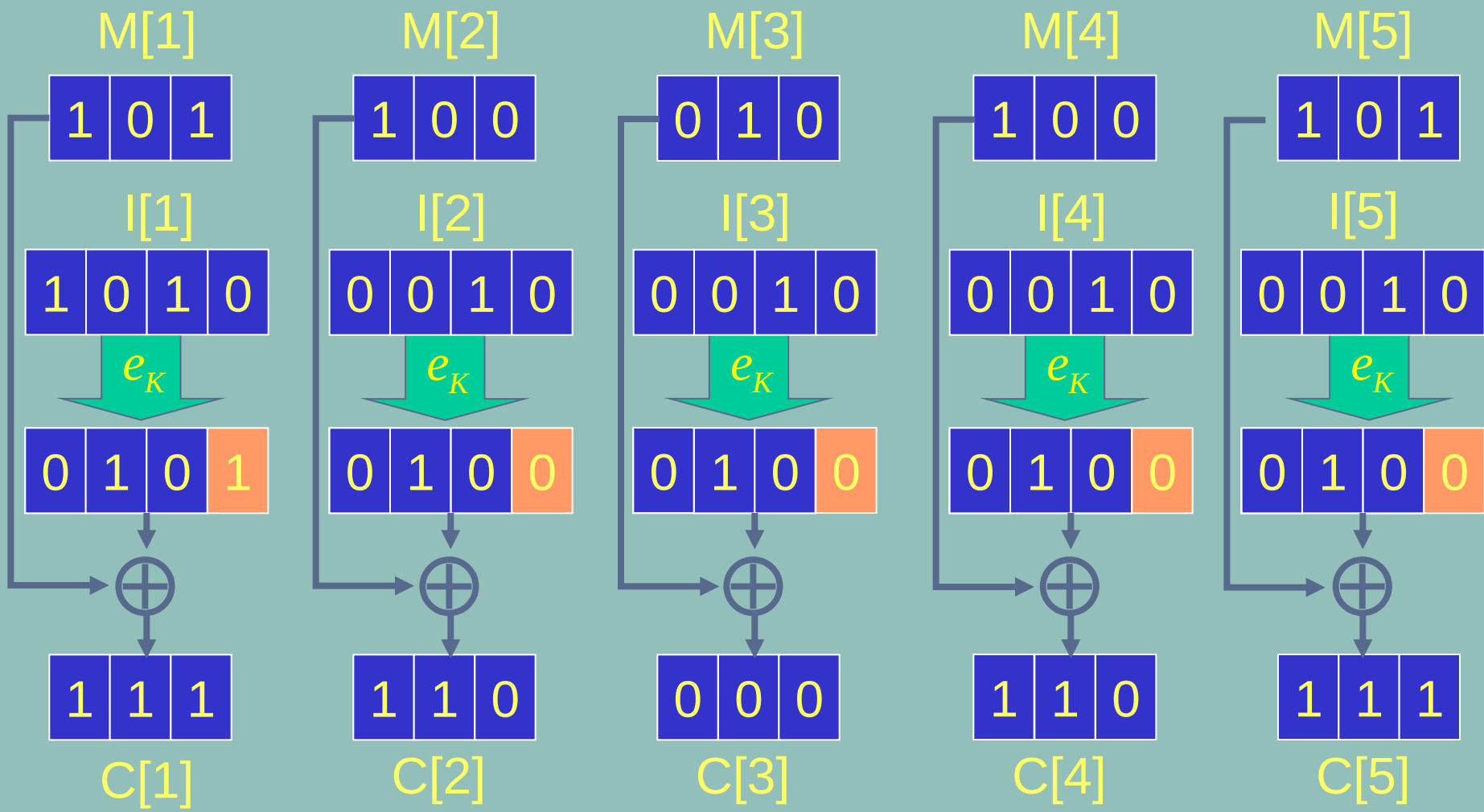
$$I[n] = \left(I[n-1] << k \right) \,|\, MSB_k\left(e(I[n-1]) \right), \text{ pour n} = 2,\ldots,N$$

$$C[n] = M[n] \oplus MSB_k\left(e(I[n]) \right), \text{ pour n} = 1,\ldots,N$$

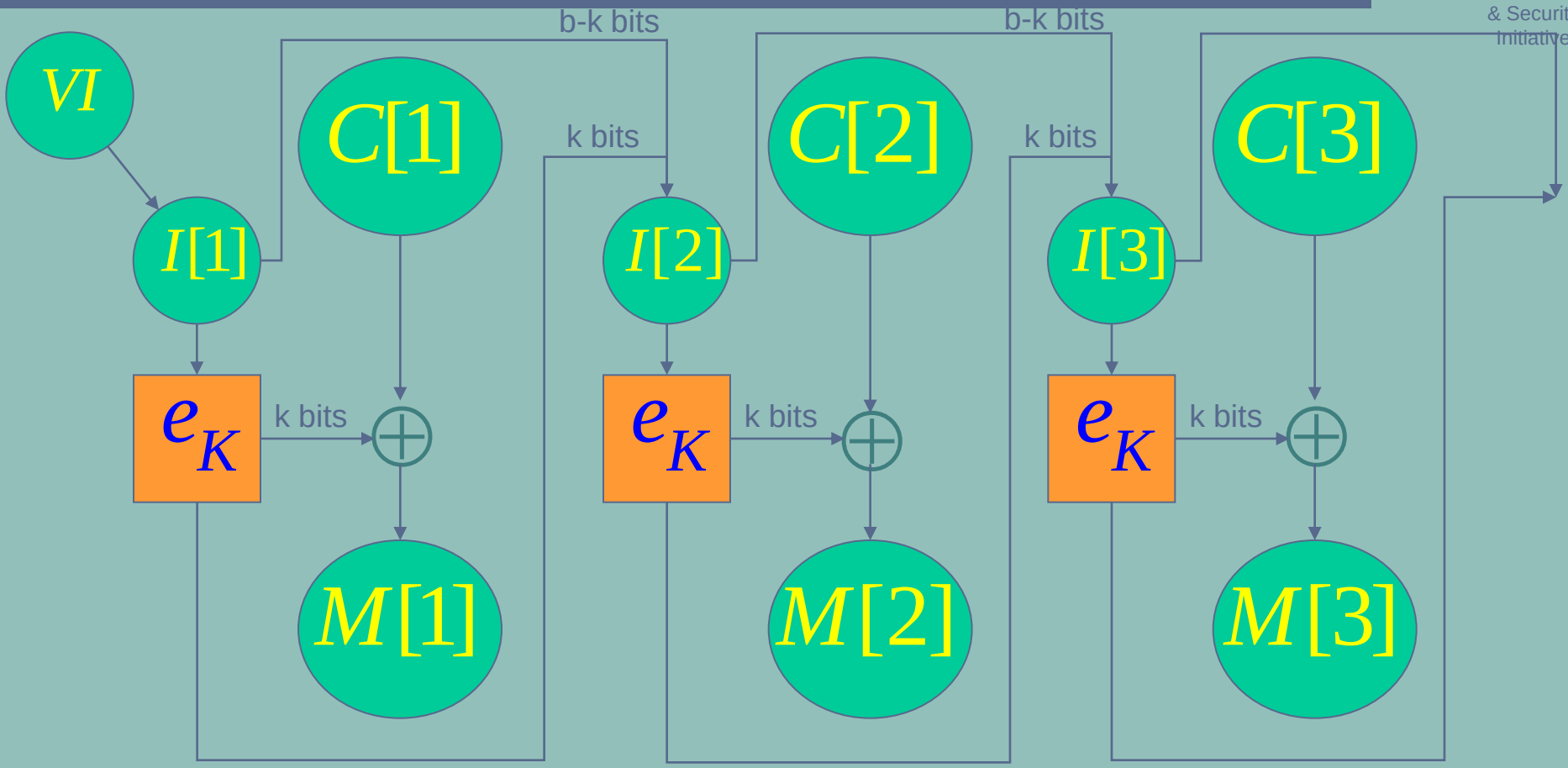
Cryptology & Security Initiative
Centre Universitaire de Luxembourg
CRP Gabriel Lippmann

Exemple en mode OFB à 3 bits (Chiffrement)

Algorithme de chiffrement : 1 2 3 4 → 2 3 4 1



Le mode OFB (Déchiffrement)



$$I[1] = VI$$

$$I[n] = \left(I[n-1] << k \right) | MSB_k \left(e(I[n-1]) \right), \text{ pour n} = 2,\ldots,N$$

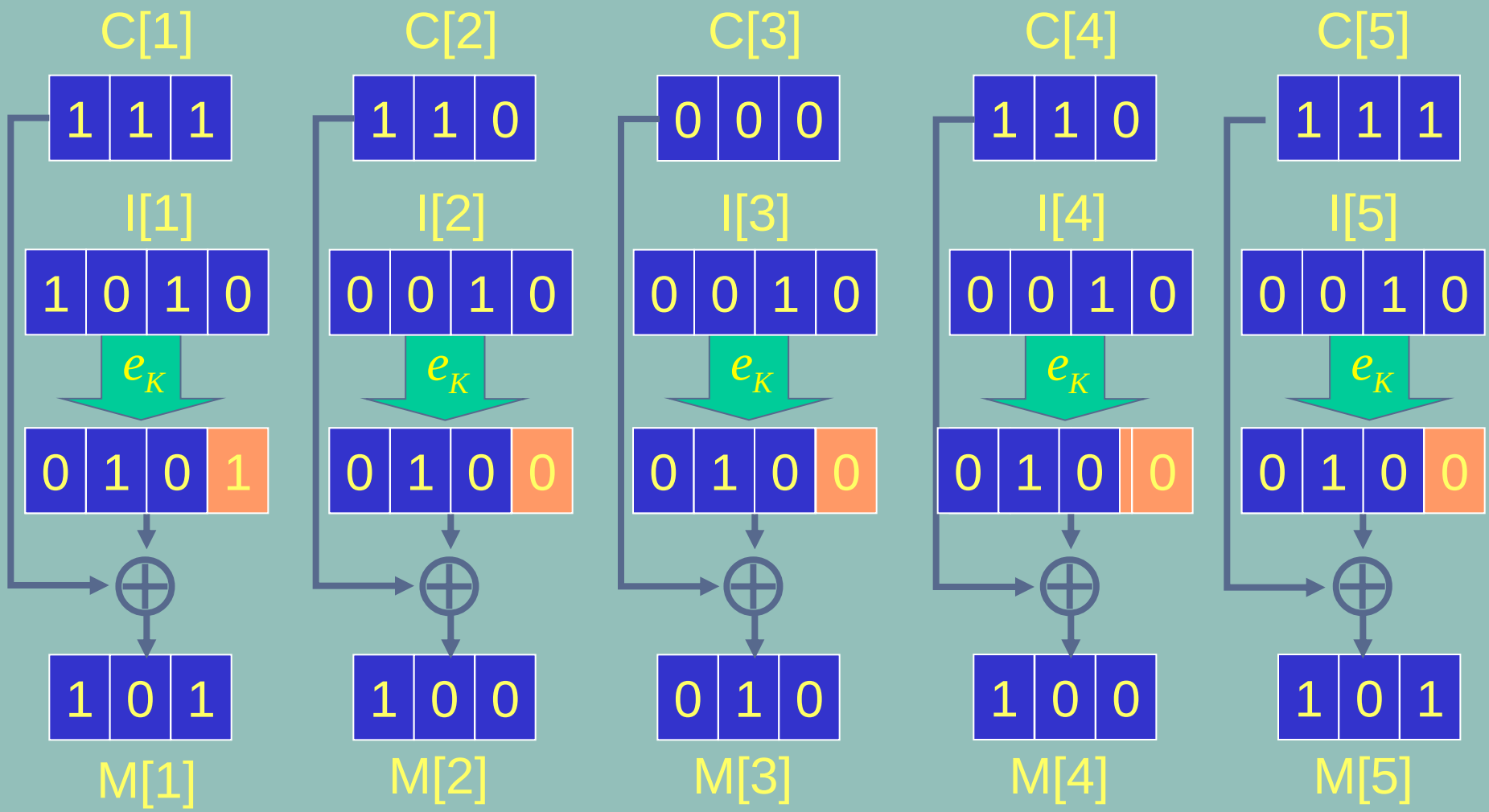
$$M[n] = C[n] \oplus MSB_k \left(e(I[n]) \right), \text{ pour n} = 1,\ldots,N$$

Centre Universitaire de Luxembourg
CRP Gabriel Lippmann

Exemple en mode OFB à 3 bits (Déchiffrement)

Cryptology & Security Initiative

Algorithme de déchiffrement : 1 2 3 4 → 4 1 2 3



Le mode OFB

Cryptology & Security Initiative

Soit b la longueur d'un bloc

Pour éviter des registres à décalage constants, on utilise le mode OFB seulement à b bits

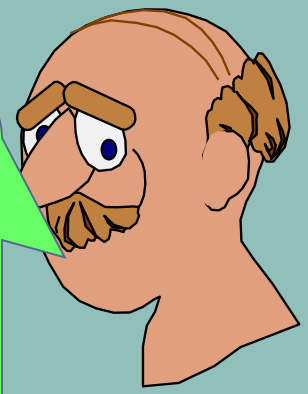
$$I[1]=VI$$

$$I[n]=e\left(I[n-1]\right), \text{ pour } n=2,\ldots,N$$

Propriétés du mode OFB

Cryptology & Security Initiative

Méthode assez Lente, mais le régistre peut être précalculé



Changer à chaque fois le vecteur d'initialisation !

Méthode souvent utilisé pour chiffrer des données synchrones à grande vitesse

Blocs de texte chiffré indépendants

Même le déchiffrement utilise uniquement l'algorithme de chiffrement

Propagation d'erreurs

Erreur d'un bit dans un bloc ⇒ Erreur d'un bit dans le texte en clair récupéré et Pas d'influence sur d'autres blocs

Erreur de synchronisation ⇒ Tout est embrouillé et Pas de rétablissement

Le mode TCBC interlacé

$$VI_1 = VI$$

$$VI_2 = VI + R_1 \pmod{2^{64}}, \text{ avec } R_1 = (5555555555555555)$$

$$VI_2 = VI + R_1 \pmod{2^{64}}, \text{ avec } R_2 = (aaaaaaaaaaaaaaaa)$$

t =1	$e_{K_1}(M_1 \oplus VI_1)$		
t =2	$e_{K_1}(M_2 \oplus VI_2)$	$d_{K_2}\left(e_{K_1}(M_1 \oplus VI_1)\right)$	
t =3	$e_{K_1}(M_3 \oplus VI_3)$	$d_{K_2}\left(e_{K_1}(M_2 \oplus VI_2)\right)$	$e_{K_3}\left(d_{K_2}\left(e_{K_1}(M_1 \oplus VI_1)\right)\right)$
t =4	$e_{K_1}(M_4 \oplus C_1)$	$d_{K_2}\left(e_{K_1}(M_3 \oplus VI_3)\right)$	$e_{K_3}\left(d_{K_2}\left(e_{K_1}(M_2 \oplus VI_2)\right)\right)$