Présentation

- Pascal PETIT
- 01 60 87 39 03 (peu joignable)
- petit@shayol.org (trop joignable)
- http://www.ibisc.fr/~petit
- Crypto: bibi
- Compression: N. Thibault

Chiffrement

- Auteur : P. Petit (pascal.petit@shayol.org)
- La bibliographie cite des sources/ressources utiles de deux catégories:
  - Des sources dont je me suis inspiré pour certains points (notamment support de cours de C. Laforest qui a assuré cet enseignement jusqu'en 2007-2008)
  - Des sources pour des approfondissements
- Les schémas/photos qui ne sont pas de moi ont en général étaient récupérés sur wikipedia

Définitions

- *Texte en clair* : un texte sous sa forme originale, compréhensible tel quel
- *Chiffrement* : transformer un texte en clair en un texte incompréhensible
- La transformation inverse quand on possède tous les éléments pour le faire s'appelle le *déchiffrement* (ne pas confondre avec décryptage)
- *Décrypter* un texte: faire de même sans avoir les éléments (clef, ...). Le correspondant légitime déchiffre le texte, l'attaquant le décrypte.

Définitions

- *cryptographie :* domaine scientifique et technique dont le but est de garder les messages secrets. Pratiquée par les cryptographes
- *cryptanalyse* : domaine scientifique et technique dont le but est de retrouver les messages en clair sans avoir tous les éléments pour le faire. Pratiquée par les cryptanalystes
- *cryptologie:* : regroupe cryptographie et cryptanalyse. Pratiquée par les cryptologues.
- *Stéganographie*: domaine scientifique et technique dont le but est de faire passer inaperçu un message dans un autre objet

Stéganographie : exemple (G. Sand à A. De Musset)

Je suis tres emue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit la une preuve que je puisse etre aimee par vous. Je suis prete a montrer mon affection toute desinteressee et sans cal- cul, et si vous voulez me voir aussi vous devoiler sans artifice mon ame toute nue, venez me faire une visite. Nous causerons en amis, franchement. Je vous prouverai que je suis la femme	sincere, capable de vous offrir l'affection la plus profonde comme la plus etroite en amitie, en un mot la meilleure preuve que vous puissiez rever, puisque votre ame est libre. Pensez que la solitude ou j'ha- bite est bien longue, bien dure et souvent difficile. Ainsi, en y songeant j'ai l'ame grosse. Accourez donc vite et venez me la faire oublier par l'amour ou je veux me mettre.

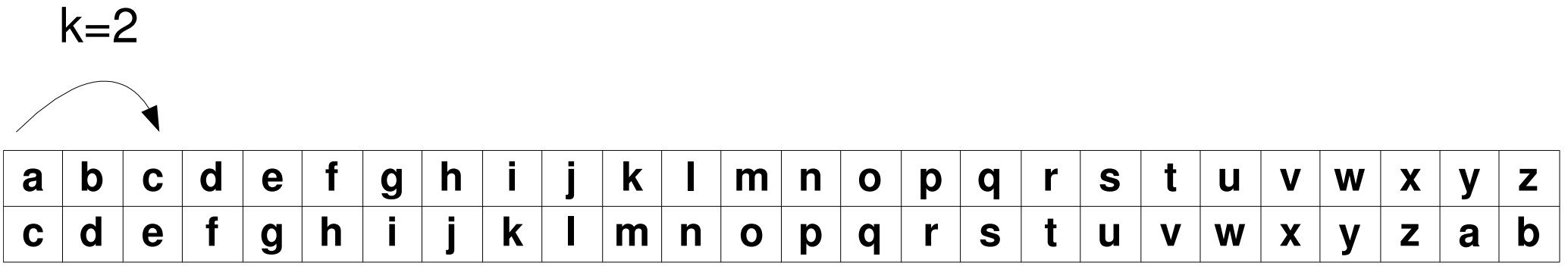
Définitions

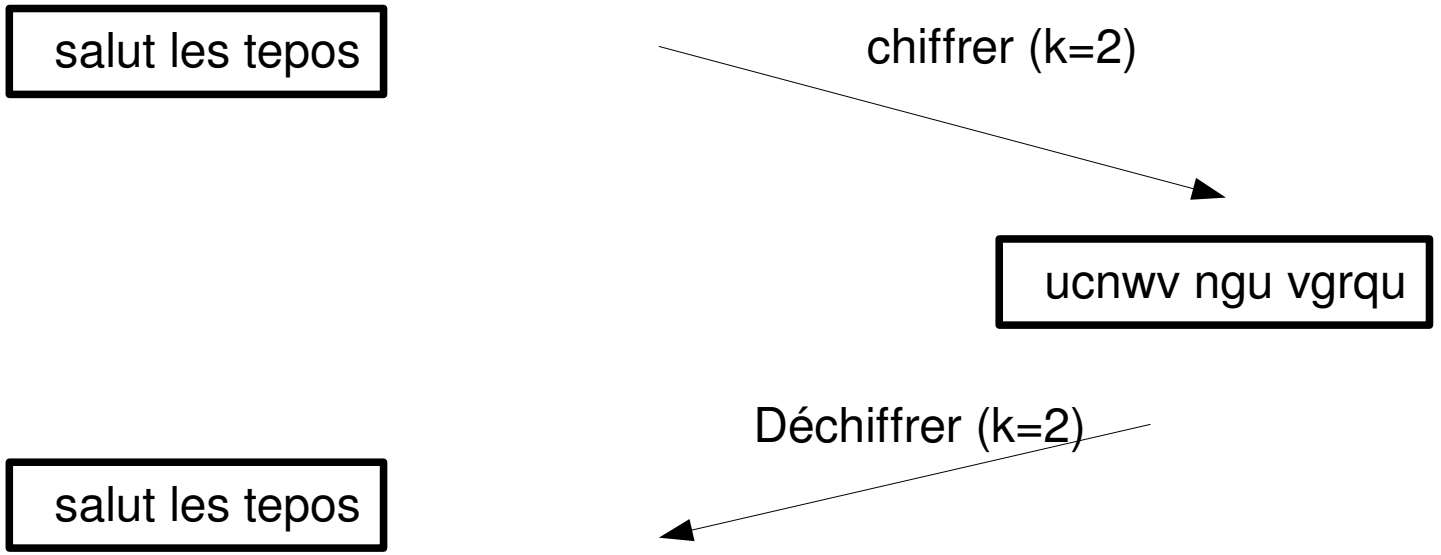
- Soit M un message en clair à faire transiter de façon sûre entre Alfred et Bachir
- Soit E le processus de chiffrement
- Soit D le processus de déchiffrement
- Alfred calcule et transmet C=E(M)
- Bachir reçoit C et doit connaître D pour retrouver M=D(C)
- On doit avoir M=D(E(M))

Historique

- L'artisanat
  - Chiffrement de césar
  - Permutation et attaque statistique
- La technique
  - ENIGMA
- Masque jetable
- L'ère scientifique (actuelle)
- Principes actuels

Chiffrement de césar





Chiffrement de césar

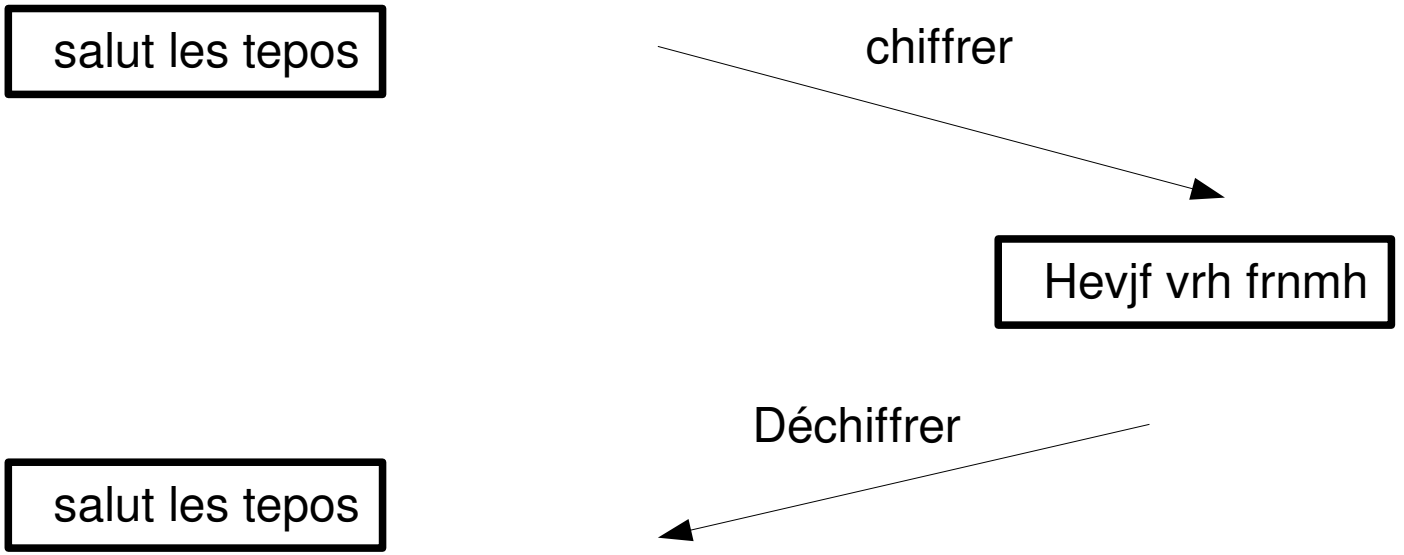
- Décaler chaque lettre de K caractères dans l'alphabet
- Exemple1: k=2 « salut les tepos » devient « ucnwv ngu vgrqu »
- Le déchiffrement se fait en décalant les lettres dans l'autre sens
- Exemple2: rot13: l'opération de codage et de décodage sont les mêmes (but: qu'un texte ne soit lu que par les gens qui souhaitent le lire. Utilisé couramment sur les forums USENET)

Chiffrement de césar

- Une fois le mécanisme est connu, la sécurité repose sur la connaissance de k
- 25 valeurs possibles pour k. Il suffit de les essayer toutes jusqu'à trouver un texte qui a un sens
- Attaque en
- brute: on essaie tout ou partie des clefs
- Ici, l'espace des clefs est trop petit

Permutation alphabétique

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
e	t	c	g	r	u	i	o	q	a	x	v	w	s	m	n	b	d	h	f	j	k	l	y	z	p



Permutation alphabétique

- On utilise une permutation quelconque de l'alphabet
- Avec un alphabet de n caractères, n ! permutations possibles
- L'espace des clefs devient très grand (26! ~ 2^88). L'attaque par force brute devient trop longue

Permutation alphabétique

- Problème: chaque lettre est toujours remplacée par la même lettre. Si on a réussit à la décoder une fois, on saura la décoder partout
- 3 attaques complémentaires possibles :
  - Parfois, de notre connaissance de la structure du message, on peut en déchiffrer certaines parties
    - On peut déchiffrer les lettres correspondantes partout dans le message
  - Attaque statistique: connaissant la langue dans laquelle le message a été écrit, on peut s'appuyer sur des statistiques d'occurences des caractères dans cette langue

Permutation alphabétique: exemple

- Sur la page WeB de ressources du cours, on vous propose un fichier chiffré à l'aide d'une permutation alphabétique
- Voir http://www.ibisc.fr/~petit
- Déchiffrez le.

Chiffrement de vigenère: substitution polyalphabétique

- Principe: chaque lettre du message est chiffré à l'aide d'un chiffrement de César avec un décalage différent;
- Pour simplifier la transmission des tables, on indique la version chiffrée de A (et on en déduit le décalage et donc les versions chiffrées des autres lettres);
- La clef est un texte indiquant la suite des versions chiffrées de la lettre A
- Un fois arrivé au bout de la clef, on repart au début

Vigénère: exemple

- Clef: tepos
- Texte à chiffrer: « ilfai tfaim »

```
i l f a i t f a i m

t e p o s t e p o s

---------------------

B P U O A M J P W E
```

- Version chiffrée: BPUOA MJPWE

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Attaques sur Vigénère

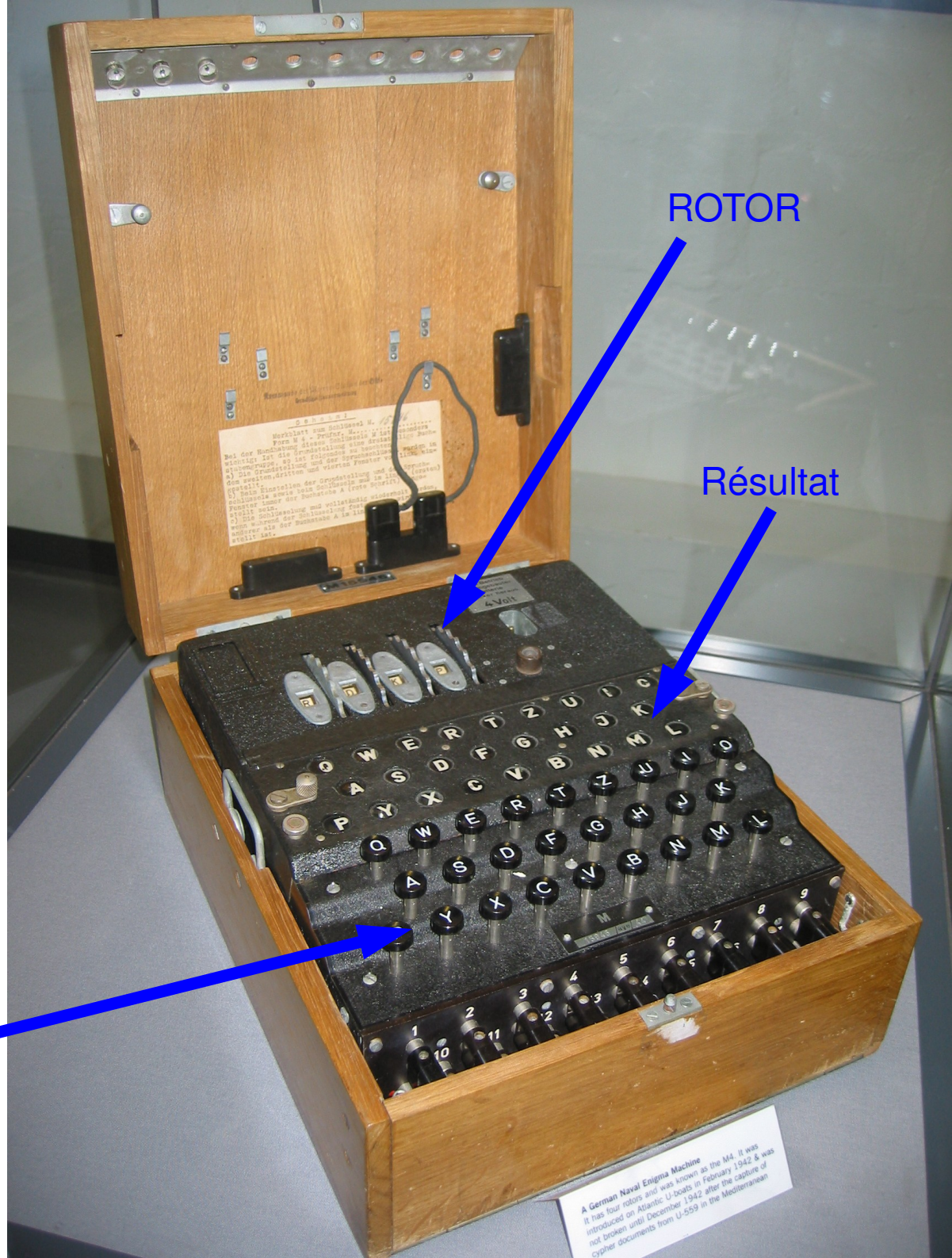
- Dans une version ultérieure de ce document

Transposition

- Transposition: changer l'ordre des lettres d'un texte
- Exemple:
  - on range le texte du message dans un tableau rectangulaire ligne par ligne
  - Le message chiffré s'obtient en lisant le tableau colonne par colonne

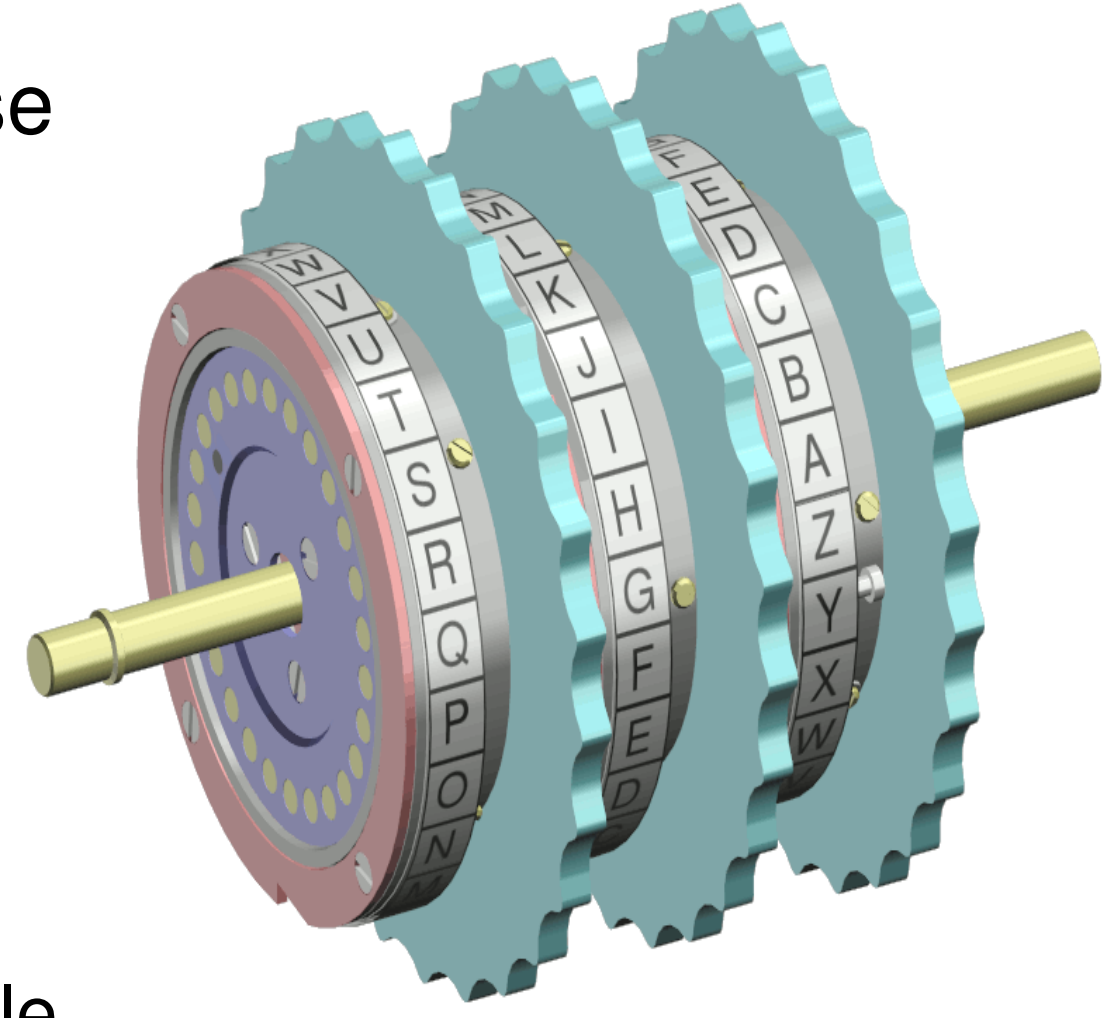
ENIGMA

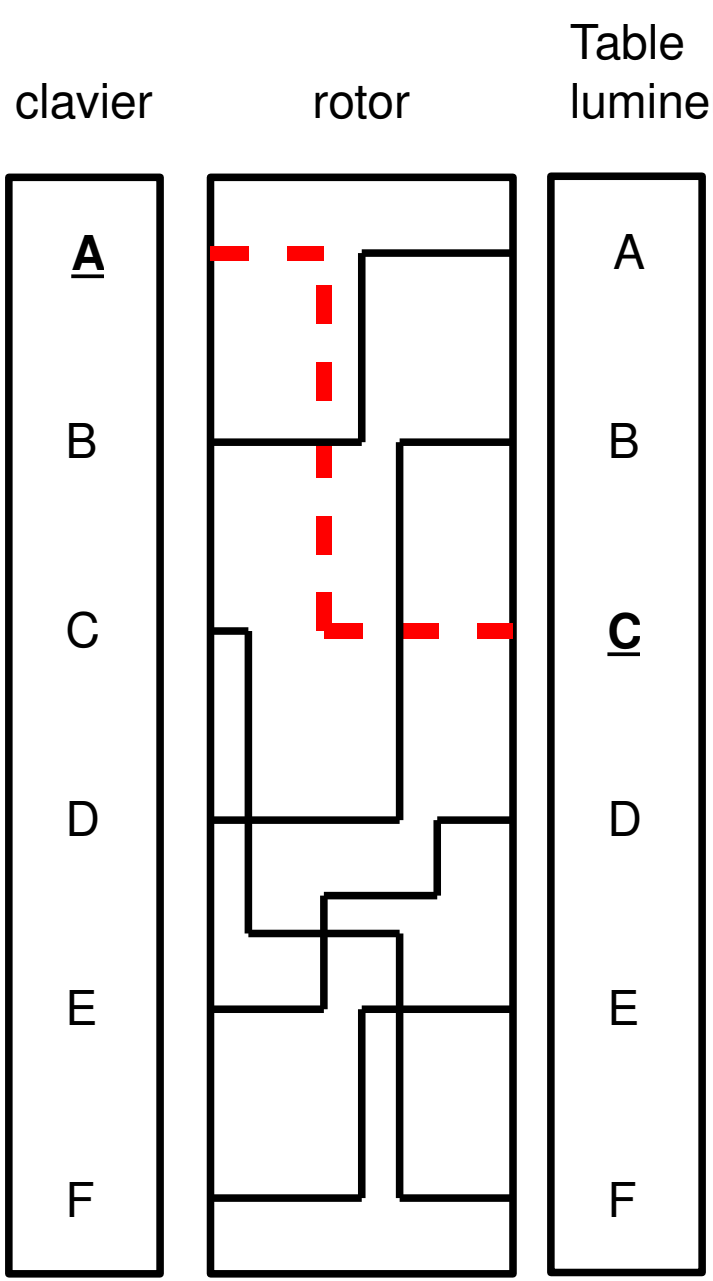
- Utilisé par les allemands durant la seconde guerre mondiale
- déchiffré par les anglais sur de longue périodes



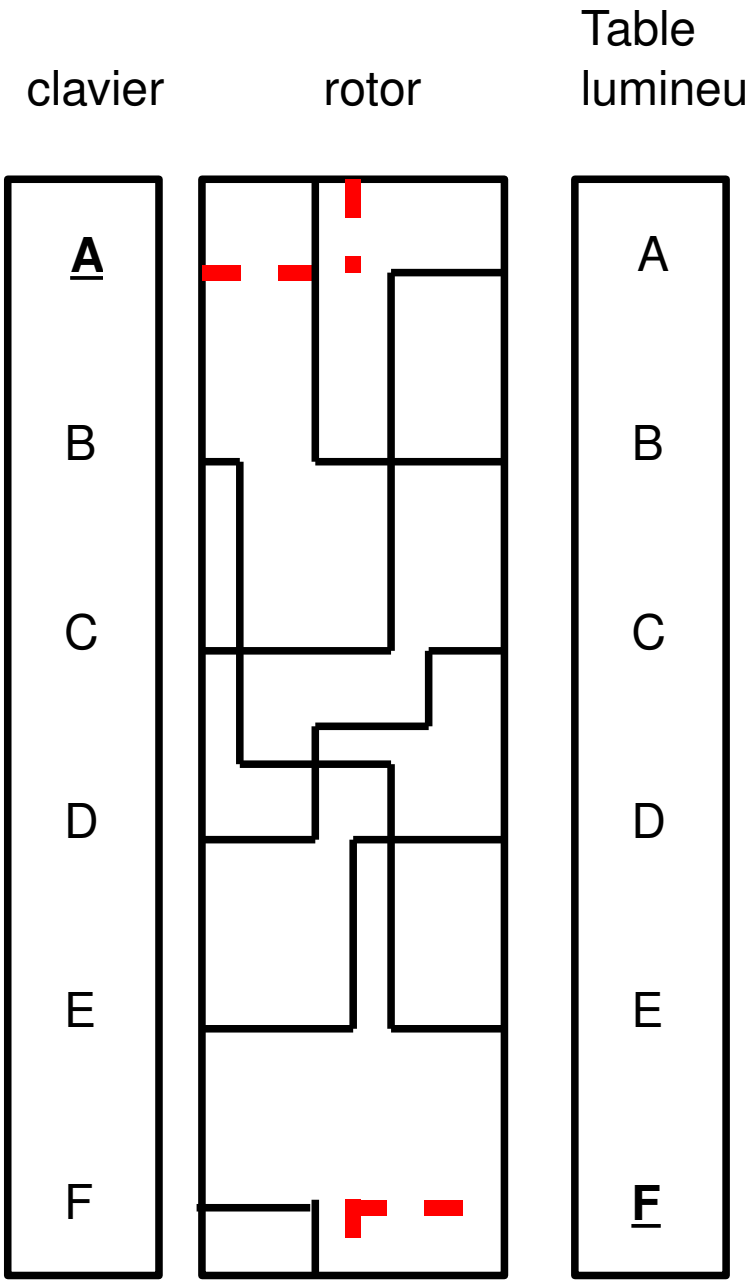
ENIGMA

- Chaque rotor réalise une substitution alphabétique
- À chaque codage d'un caractère,
  - le premier rotor tourne
  - Quand le premier rotor a fait un tour, le second rotor tourne
  - ...





Enigma



Enigma après avancement du rotor d'un cran

Enigma

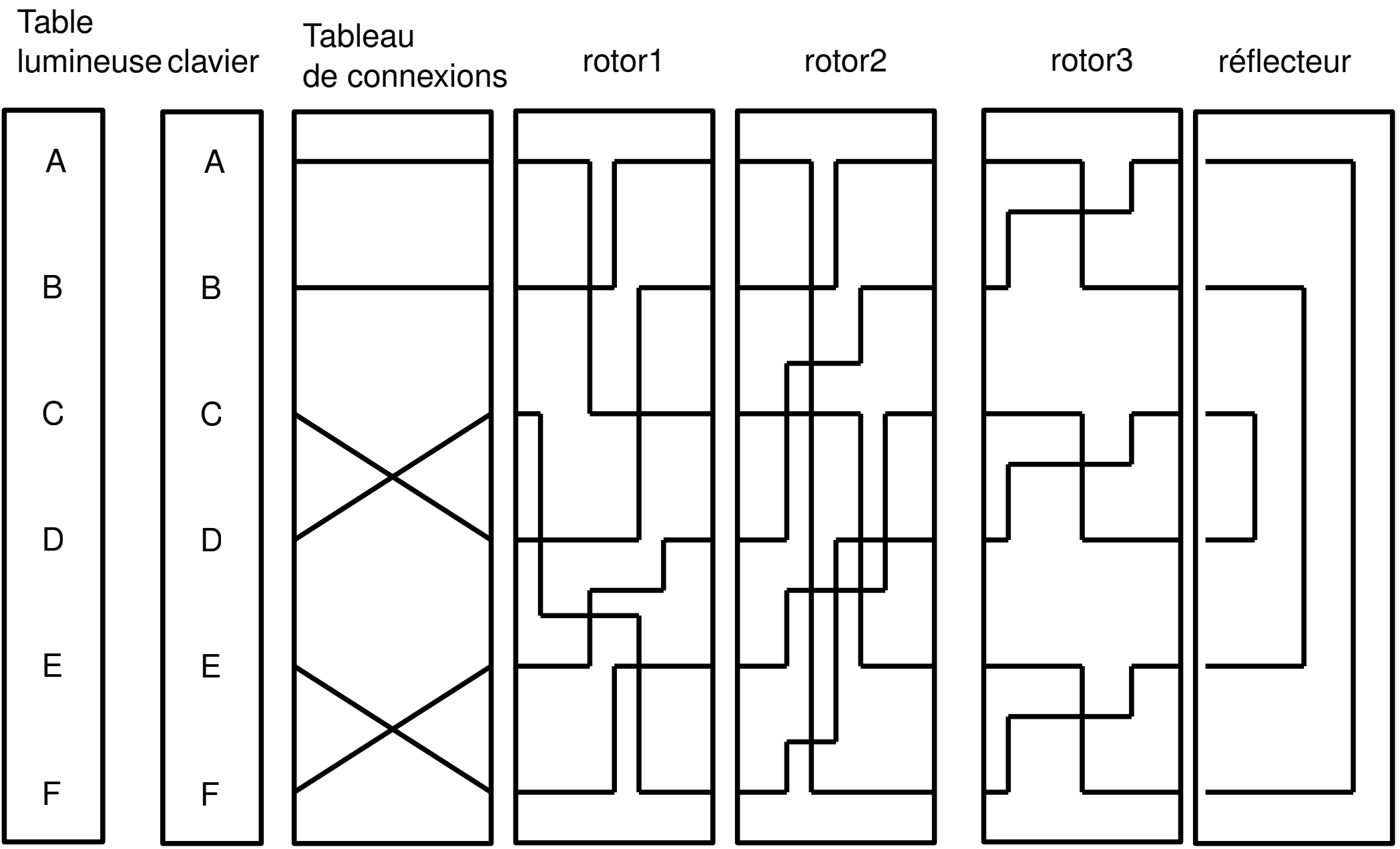
- Conséquence :
  - Les substituions changent donc à chaque caractère codé
  - Il faut que tous les rotors aient fait un tour complet pour qu'on retrouve la même transformation
    - Avec un rotor alphabétique, il faudrait 26 mouvements pour revenir à la transformations initiale
    - Avec deux rotors, 26*26
    - Avec n rotor 26^n
  - Les attaques sur vigenere ont montré la faiblesse que constituait de la répétition des transformations
  - Là, on les limite à défaut de les supprimer

ENIGMA: nature et nombre des clefs

- Clef:
  - Le choix de la position des rotors (un rotor = une permutation): 6 possibilités
  - La position initiale des rotors => 26^3=17576 clefs
- Ça fait beaucoup pour des attaques manuelles
- Plus tard: jusqu'à 8 rotors + choix des rotors
- Un mécanisme de permutations de 6 fois 2 lettres multiplie le nombre de possibilités par 100 391 791 500
- => espace de clef très grand = #10^{16}

ENIGMA: transpositions

- Pour compliquer :
  - ajout d'un étage de transposition permettant d'échanger deux lettres: ENIGMA avait 6 mécanismes permettant l'échange de 2 lettres au choix
  - Ajoute 100 391 791 500 possibilités = C(26,12)*11*9*7*5*3*1
    - C(26,12): choisir 12 lettres parmi 26 sans tenir compte de l'ordre
    - Ensuite, on choisir la lettre qu'on associe à la première: 11 possibilités.
    - Il reste 10 lettres disponible.On fait de même pour la première de ces 10 lettres: reste 9 possiblités
    - ...



Permutations: 2 permutations de 2 lettres dans notre exemple

Réflecteur: codage et décodage sont une seule et même opération

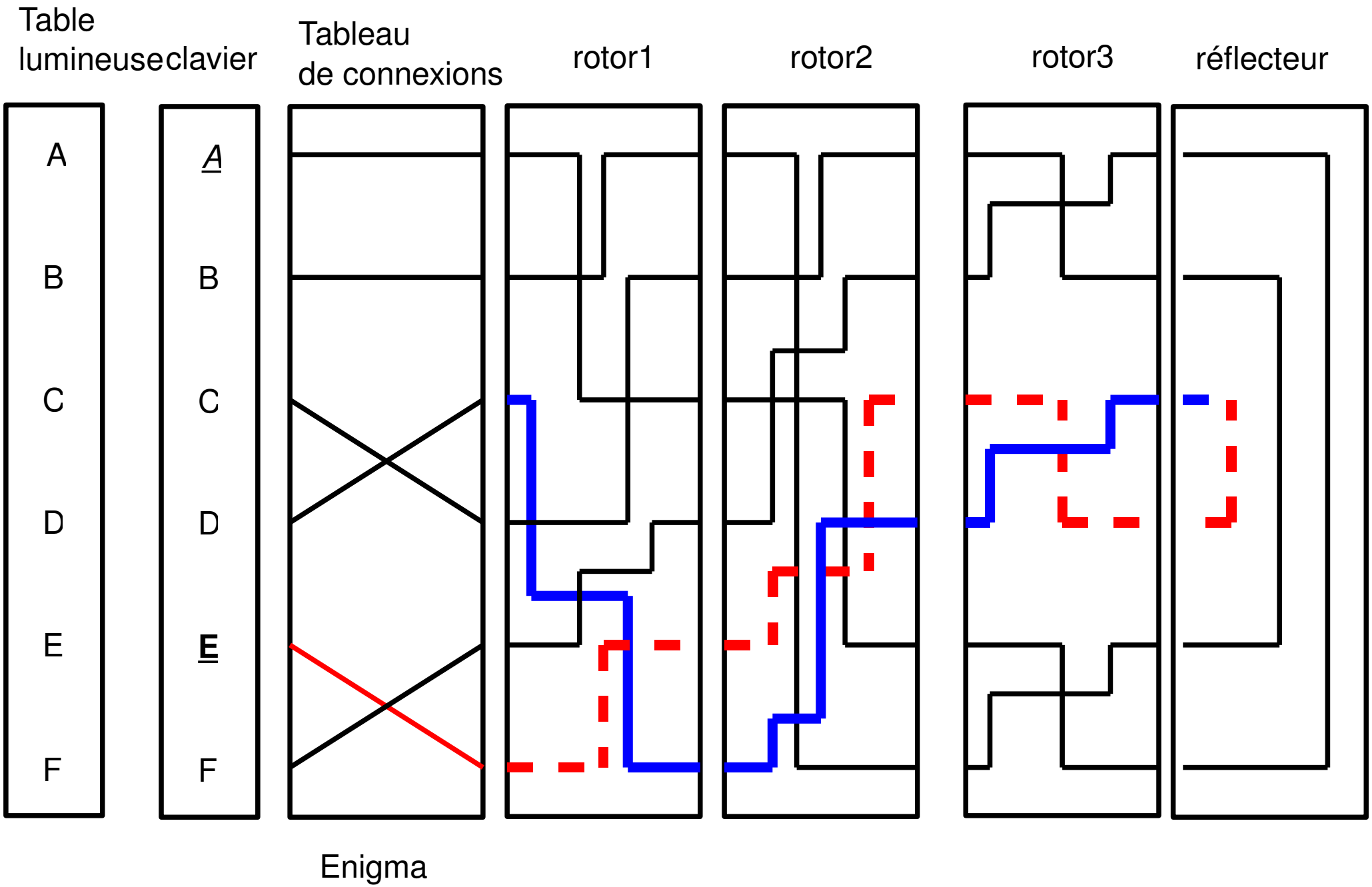


Table lumineuse
clavier
Tableau de connexions
rotor1
rotor2
rotor3
réflecteur
A
B
C
D
E
F
A
B
C
D
E
F
Enigma

Décryptage d'ENIGMA

- Dans une version ultérieure de ce document.

Masque jetable

- Principe du tel. Rouge entre URSS et USA
- Soit M un message binaire=b1b2b3...bl (avec l le nombre de bits du message)
- Soit K=k1k2k3...kl une suite de bits impossibles à prédire (on utilise une suite tirée aléatoirement)
- Pour obtenir le message chiffré, on fait un où exclusif entre chaque bit du message et celui de la clef
  - $c_i = b_i$ XOR k_i

Masque jetable

- Table du XOR: 0 XOR 0=0, 1 XOR 0 = 0 XOR 1 = 1 et 1 XOR 1 = 0
- Avantages du masque jetable:
  - Simple à mettre en oeuvre, rapide
  - Sûr si la clef est imprévisible
- Défauts :
  - Transport de la clef: les deux extrémités doivent l'avoir mais pas l'espion. Le transfert sûr de la clef est aussi difficile que celui du message.
  - La génération de la clef qui ne peut être réutilisée d'un message à un autre

Masque jetable

- Connaissant le message et sa version chiffrée, on peut en déduire facilement la clef K
- C= M XOR K
- K = M XOR C
- Conséquence: il faut une nouvelle clef pour chaque message
- Méthode du masque jetable ou « One Time Pad »

Principes de Kerckhoffs

- Auguste Kerckhoffs (Hollande, 1883)
  - Seule une donnée de petite taille (clef) doit suffire à assurer la sécurité
  - La sécurité d'un mécanisme ne doit pas reposer sur son caractère secret
- Il est beaucoup plus facile de garder secret un clef connue d'une personne qu'un procédé mis au point par plusieurs personnes.

L'ère scientifique:

- 1976: Diffie et Hellman découvrent la crypographie à clef publique en mettant au point un algorithme d'échange de clefs ne supposant aucun échange de secret préalable
- 1977: DES (standard américain de chiffrement symétrique)
- 1978: Rivest, Shamir et Alderman (re)découvrent RSA (système dechiffrement à clef publique)

algorithme de chiffrement symétrique (à clefs privées)

- Chiffrement symétrique:
  - la même clef sert au chiffrement et au déchiffrement
  - C'est le principe du coffre fort:
    - Akira et Barack connaissent tous deux la combinaison du coffre fort :
      - Akira dépose un message dans le coffre fort en utilisant la combinaison : elle chiffre le message avec la clef partagée
      - Barack récupère le message en ouvrant le coffre avec la même combinaison: il déchiffre le message avec la clef partagée
      - Si une autre personne réussit à avoir la combinaison, il peut lui aussi ouvrir le coffre et lire ou déposer des messages: elle peut chiffrer de nouveaux messages ou déchiffrer les messages transmis

Chiffrement symétrique

- les algo classiques sont rapides
- Pb:
  - comme faire en sorte que Bob et Alice connaissent la clef ?
  - Problème loin d'être négligeable qui se coûtait des sommes importantes aux services secrets du monde entier pour diffuser et renouveler les clefs secrètes envoyées à leur agents :
    - Renouveler suffisamment souvent les clefs
    - Avoir une clefs spécifique pour chaque contexte/agent pour éviter les conséquences de la récupération d'une clef par l'ennemi

algorithme de chiffrement

- chiffrement asymétrique:
  - Chaque participant x
    - a une clef publique Px qu'il peut diffuser à tous
    - A une clef secrète Qx qu'il doit être seul à connaître
  - Le chiffrement se fait avec la clef publique
  - Le déchiffrement se fait avec la clef privée
  - Principe de la boîte aux lettres :
    - Alice peut déposer des messages dans la boîte aux lettres: elle chiffre un message avec la clef publique
    - Bob est le seul à avoir la clef de la boîte aux lettre et donc le seul à pouvoir lire les messages qui y ont été déposés: il est seul à pouvoir déchiffrer des messages avec la clef privée.
  - Exemple: si Alice veut envoyer un message à Bob
    - Elle chiffre le message avec la clef publique de Bob
    - Bob reçoit le message chiffré et le déchiffre avec sa clef privée
  - les algo classiques sont lents

algorithmes classiques

- symétriques:
  - DES (1976): standard américain (1977), clef de 56 bits sur des blocs de 64 bits. dépassé de nos jours.
  - triple DES (1978): variante, triple application de DES, clefs entre 128 et 192 bits sur des blocs de 64 bits.
  - RC2, RC4, RC5 (1994) et RC6:
  - IDEA (1992): clef 128 bits sur des blocs de 64 bits
  - blowfish: clef 32 à 448 bits sur des blocs de 64 bits. Algo très analysé,considéré comme solide. utilisation libre.
  - AES (1998): clefs 128, 192 ou 256 bits sur blocs de 128 bits. standard américain. utilisation libre.

algorithmes classiques

- asymétriques:
  - RSA s'appuyant sur la factorisation de nombres premiers
  - Diffie-Hellman et El Gamal s'appuyant sur le calcul des logarithmiques discrets
  - des algorithmes nouveaux s'appuyant sur les courbes elliptiques

Système hybrides

- On génère une clef de session Ks
- On utilise un chiffrement à clef publique pour la transmettre à son correspondant
- On chiffre le reste de la communication avec un algorithme symétrique (donc rapide) utilisant la clef Ks

L'espion

- L'espion est un personnage classique de la cryptographie. Le but initial de la cryptopgraphie était de protéger des communications de ses actions :
  - Il peut vouloir écouter et déchiffrer un message
  - Il peut vouloir déchiffrer tous les messages échangés entre Ahmed et Bernard
  - Il peut vouloir modifier les messages entre Arthur et Bérénice (on parle alors d'écoute active)

L'espion (2)

- Il peut se faire passer pour Anas auprès de Bérénice: on parle d'usurpation d'identité
- Il peut se faire passer pour Alex auprès de Bertrand et pour Bertrand auprès d'Alex : attaque « Man In the Middle »
- Bertrand peut refuser de reconnaître être l'auteur d'un message (reconnaissance de dette, ...) qu'il a pourtant envoyé à Aïcha.

Services s'appuyant sur de la cryptographie

- Confidentialité
- Intégrité
- Authentification:
- Non répudiation

Confidentialité

- protection des données contre une divulgation non autorisée
- 2 moyens techniques complémentaires
  - protéger l'accès aux données (implique authentification et contrôle d'accès). Ex.: authentification windows + ACL NTFS
  - les chiffrer
- intégrité, confidentialité : des contraintes opposées
  - intégrité : multiplier les sauvegardes notamment hors site
  - confidentialité: limiter les lieux de stockage pour faciliter le contrôle d'accès

Intégrité

- certifier que les données n'ont pas été altérées de façon intentionnelle ou accidentelle
- la modification peut avoir lieu
  - lors du transfert des données (corruption, écoute active)
  - lors du stockage des données
  - lors de leur traitement (bogues des logiciels applicatifs, des OS).
- Implications:
  - légales, plantage des applications et perte d'activité
  - perte d'image

Identification et authentification

- **identification**: définir l'identité de l'utilisateur
- **authentification**: permet de vérifier l'identité fournie (authentification simple vs authentification forte)
  - via un élément que l'utilisateur connait (mot de passe, ...)
  - via un élément que l'utilisateur possède (carte à puce, certificat, ...)
  - via biometrie

authentification

- élément clef pour assurer :
  - la confidentialité et l'intégrité des données via un contrôle d'accès: seules les personnes identifiées, authentifiées et habilités à le faire peuvent accèder/modifier les données
  - la non-répudiation et l'imputabilité (preuve d'une transaction, ...)
- Authentification unique (SSO: Single Sign On)
  - l'utilisateur s'authentifie une fois
  - il a accès à toutes les ressources du réseau
  - cf partie technique (keberos, ...)

non répudiation

- **non répudiation** : ne pouvoir nier qu'un événement a eu lieu
- **imputabilité**: on sait qui a réalisé une action
- **traçabilité**: mémoriser des événements imputables
- **auditabilité**: pouvoir réaliser une analyse ultérieure d'un événement. Ex.: en cas d'intrusion.
- moyens: utilisation de journaux
  - de taille limitée
  - éventuellement hors site (intrusion)

Signature électronique

- Définition: la *signature électronique* a pour objectif de permettre à une personne d'attacher son identité à un message.
- Problèmes:
  - Le message doit être protégé contre les modifications sinon que certifie-t-on en le signant ?
  - La signature ne doit pas pouvoir être utilisée pour signer un autre message

Signature électronique: exemple à ne pas suivre

- Supposons que signer se résume à ajouter son nom à la fin d'un fichier
  - Tout le monde peut imiter une telle signature (pb de non répudiation)
  - Le document signé peut-être modifié (ajoutons un zéro sur la somme citée dans un chèque et changeons le bénéficiaire)
  - Ajouter de l'information à la fin d'un fichier peut le corrompre

Signature:

- Elle se décompose en deux parties:
  - Un procédé de signature: permet d'obtenir les données signées.
    - Ne doit pouvoir être appliqué que par le signataire.
    - Utilise en général un secret détenu par le signataire
  - Un procédé de vérification: à partir d'un texte signé et de l'identité du signataire, le procédé de vérification doit confirmer que le texte signé a bien été signé par le signataire désigné
    - doit pouvoir se faire sans secret détenu par le signataire.
- Signature et confidentialité sont deux services distincts qui sont parfois intégrés dans un même système.

Chiffrement symétriques

- clef de chiffrement = clef de déchiffrement
- Chiffrements par bloc:
  - DES (1977), blocs de 64 bits, clefs de 56 bits
  - IDEA (Lai Massey 1991), blocs de 64 bits, clefs de 128 bits
  - Rinjdael (Rinmen, Daemen, 1997): blocs de 128 ou 256 bits, clefs de 128, 192 ou 256 bits
  - AES, blocs de 128 bits, clefs de 128, 256 bits
- Chiffrement en continu d'un flux
  - RC4: chiffrement octets par octets
  - Pseudo-Vernam: XOR entre le flux et la sortie d'un générateur aléatoire

Principes de conception

- Problème :
  - On connaît de nombreux systèmes faibles (cesar, substitution, vigenere, ...)
  - comment construire des systèmes sûrs et plus efficaces que le masque jetable

Principes de conception

- Claude Shannon, 1949, « Communication Theory of Secrecy Systems »
  - Confusion: la relation entre le texte clair et le message chiffré doit être impossible à établir. Ca doit notamment être le cas pour les propriétés statistiques de l'un et de l'autre
  - Diffusion: un bit de clef ou de texte clair doit influencer de nombreux bits du texte chiffré.

Chiffrement symétrique : modes de chiffrement

- Chiffrement par bloc:
  - L'algo de chiffrement est capable de chiffrer des blocs de taille fixe
  - découper le message en bloc et chiffrer chaque bloc
  - Plusieurs modes opératoires peuvent être employées (voir plus loin: ECB, CBC, ...)
- Chiffrement en continu
  - On chiffre le texte en clair au fur et à mesure qu'il se présente
  - Utile dans le cadre d'application réseau
  - Une solution: utiliser la technique du masque jetable avec des masques précalculés ou calculés au vol à partir d'une clef de base

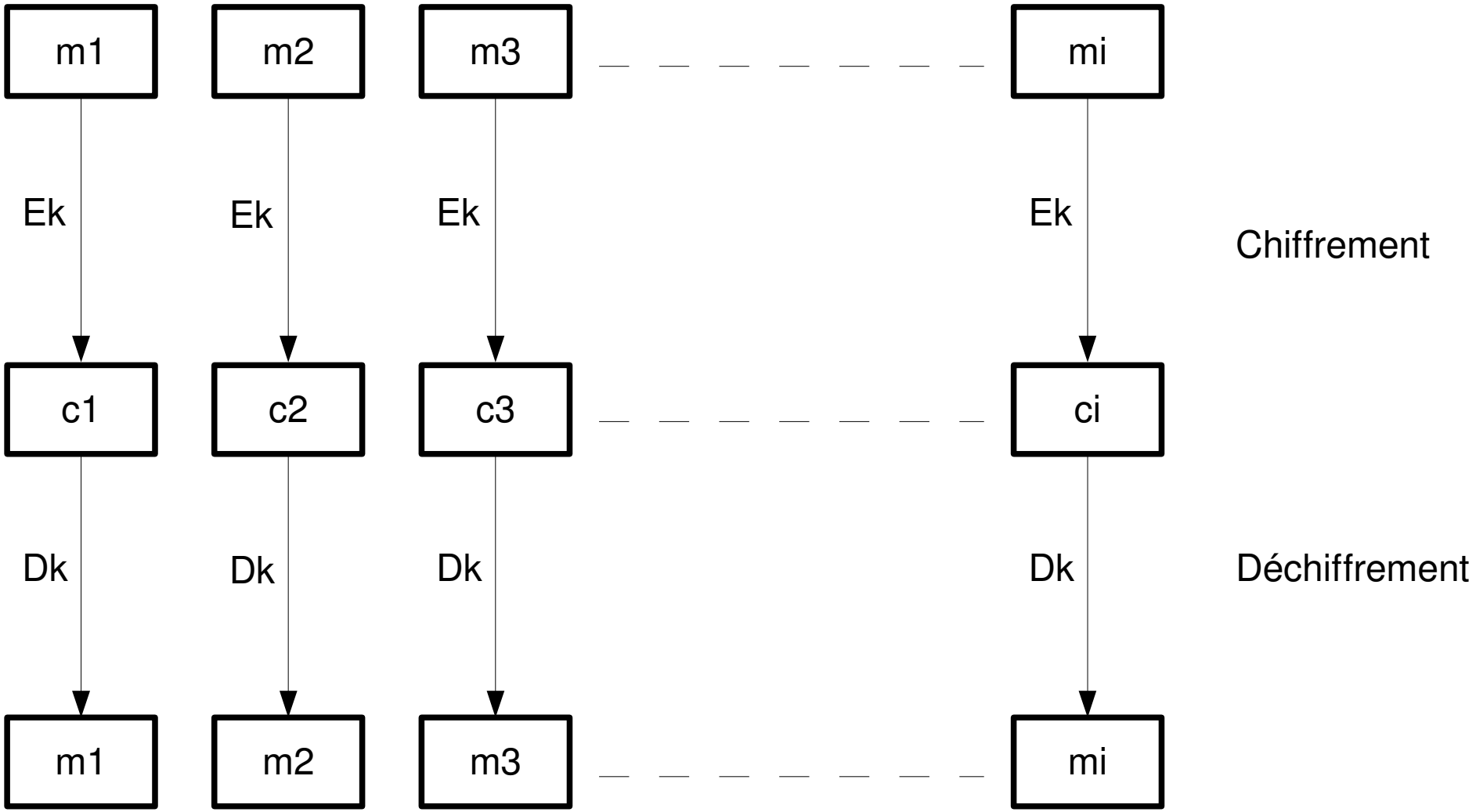
Chiffrement par bloc: ECB

- Electronic code Book (ECB) : on chiffre chaque bloc indépendamment des autres
  - Soit m le message en clair: $m=m_1 m2_{...} m_p$
  - c la version chiffrée de m: $c=c_1 c_{2...} c_p$
  - E une fonction de chiffrement capable de chiffrer des blocs, D la fonction de déchiffrement associée
  - K une clef de chiffrement pour E, déchiffrement pour D
- ECB:
  - Chiffrer: $c_1=E(m_1, k)$, $c_2=E(m_2, k)$, ..., $c_p=E(m_p, k)$
  - Déchiffrer: $m_1=D(c_1)$, $m_2=D(c_2)$, ..., $m_p=D(c_p, k)$

Chiffrement par bloc: ECB

- ECB:
  - Chiffrer: $c_1=E(m_1, k)$, $c_2=E(m_2, k)$, ..., $c_p=E(m_p, k)$
  - Déchiffrer: $m_1=D(c_1)$, $m_2=D(c_2)$, ..., $m_p=D(c_p, k)$
- On suppose que c2 est verollé: c'2. Quelle conséquence sur le déchiffrement :
  - m1=D(c1) : OK; D(c'2) ne donne **m2**
  - m3=D(c3) : OK, m4=D(c4): OK

Chiffrement par bloc: ECB



Chiffrement par bloc: ECB

- Electronic code Book (ECB) : on chiffre chaque bloc indépendamment des autres
  - Avantage:
    - Simple
    - On peut modifier un morceau des données sans modifier toutes la version chiffrée
    - On peut précalculer les versions chiffrées des blocs pour gagner en vitesse

Chiffrement par bloc: ECB

- Electronic code Book (ECB) : on chiffre chaque bloc indépendamment des autres
  - Défaut: mauvaise sécurité
    - Un bloc sera tout le temps chiffré de la même manière à l'intérieur d'un message ou dans des messages différents avec la même clef
    - L'espion peut se faire un dictionnaire s'il arrive à obtenir les versions chiffrées et en clair de certains message
  - Amélioration:
    - Ajouter un texte aléatoire avant chaque bloc à chiffrer
    - Le retirer au déchiffrement
    - Défaut: on augmenter la taille des données à chiffrer ce qui peut poser des problèmes de performances

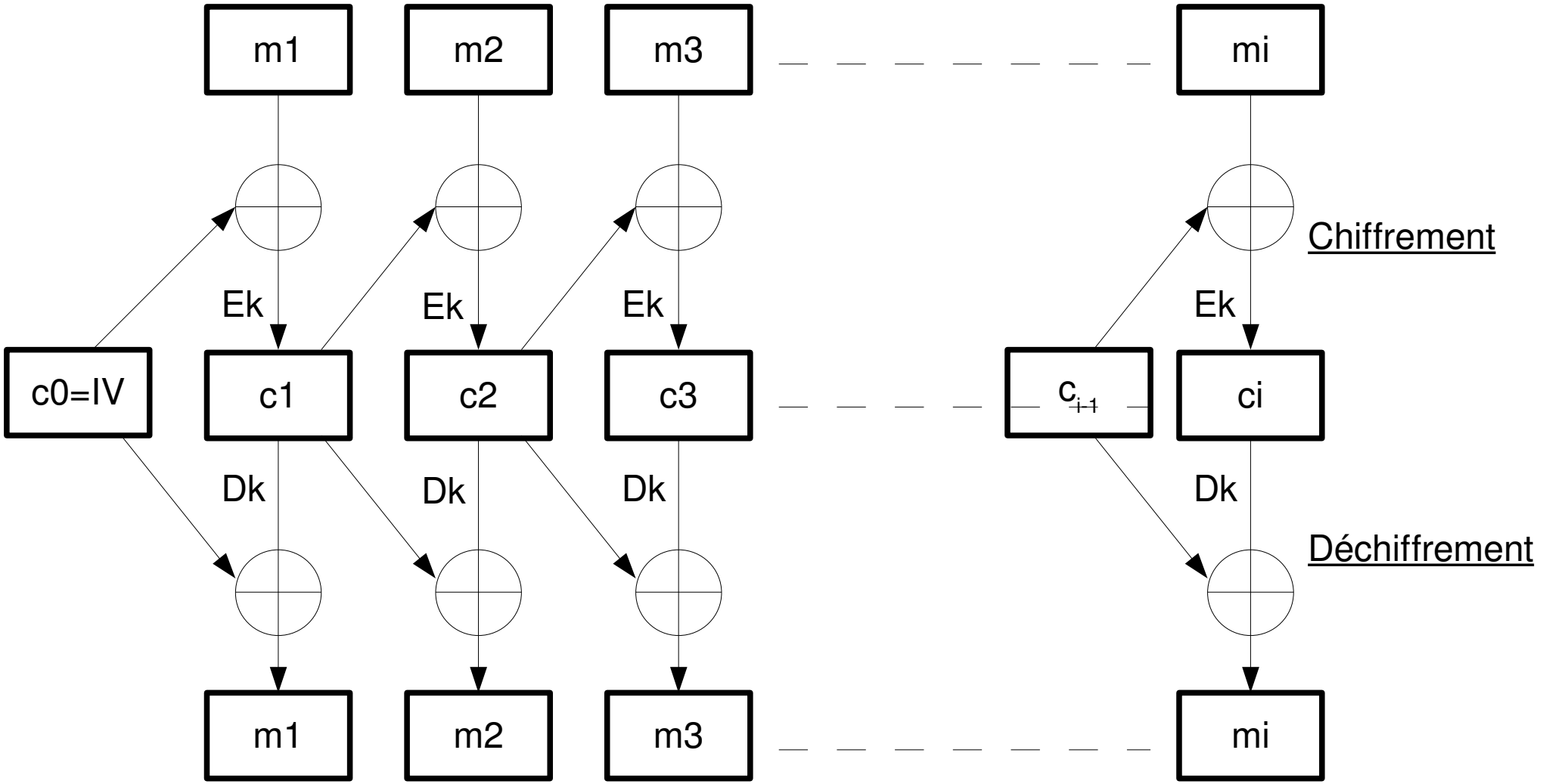
Chiffrement par bloc: CBC

- Cypher Bloc Chaining : les blocs sont chiffrés en fonction les uns des autres.
  - En mode CBC: le texte en clair est combiné par un XOR avec la version chiffrée du bloc précédent
  - 2 messages avec le même début et chiffrés avec la même ont leur version chiffrée qui commence pareil :
    - Solution : On ajoute un premier bloc aléatoire IV (vecteur d'initialisation)Cet IV est transmis en clair.
  - Avantage:
    - sûr
  - Défaut:
    - Une erreur rend illisible toute la suite des données
    - Peformance: Non parallélisable

Chiffrement par bloc: CBC

- CBC :
  - Chiffrer:
    - c_0=IV,
    - c_1=E($c_0 \oplus m_1$,k),
    - c_2=E($c_1 \oplus m_2$,k), ...,
    - c_p=E($c_{p-1} \oplus m_p$,k)
  - Déchiffrer:
    - c_0=IV,
    - m_1=$c_0 \oplus$D(c_1,k),
    - m_2=$c_1 \oplus$D(c_2,k), ...,
    - m_p=$c_{p-1} \oplus$D(m_p,k)

Chiffrement par bloc: CBC



Chiffrement par bloc: OFB

- Mode OFB (Output Feedback) ou à rétroaction de sortie
  - E: chiffrement de blocs de longueur n
  - $1 \leq r \leq n$
  - Un vecteur d'initialisation IV
  - On découpe les données à chiffrer en blocs de taille r
- Chiffrement:
  - I_1=IV
  - O_j=E(I_j,k)
  - t_j les r premiers bits de O_j
  - c_j= $m_j \oplus t_j$
  - I_{j+1}=O_j

Déchiffrement:

I_1=IV

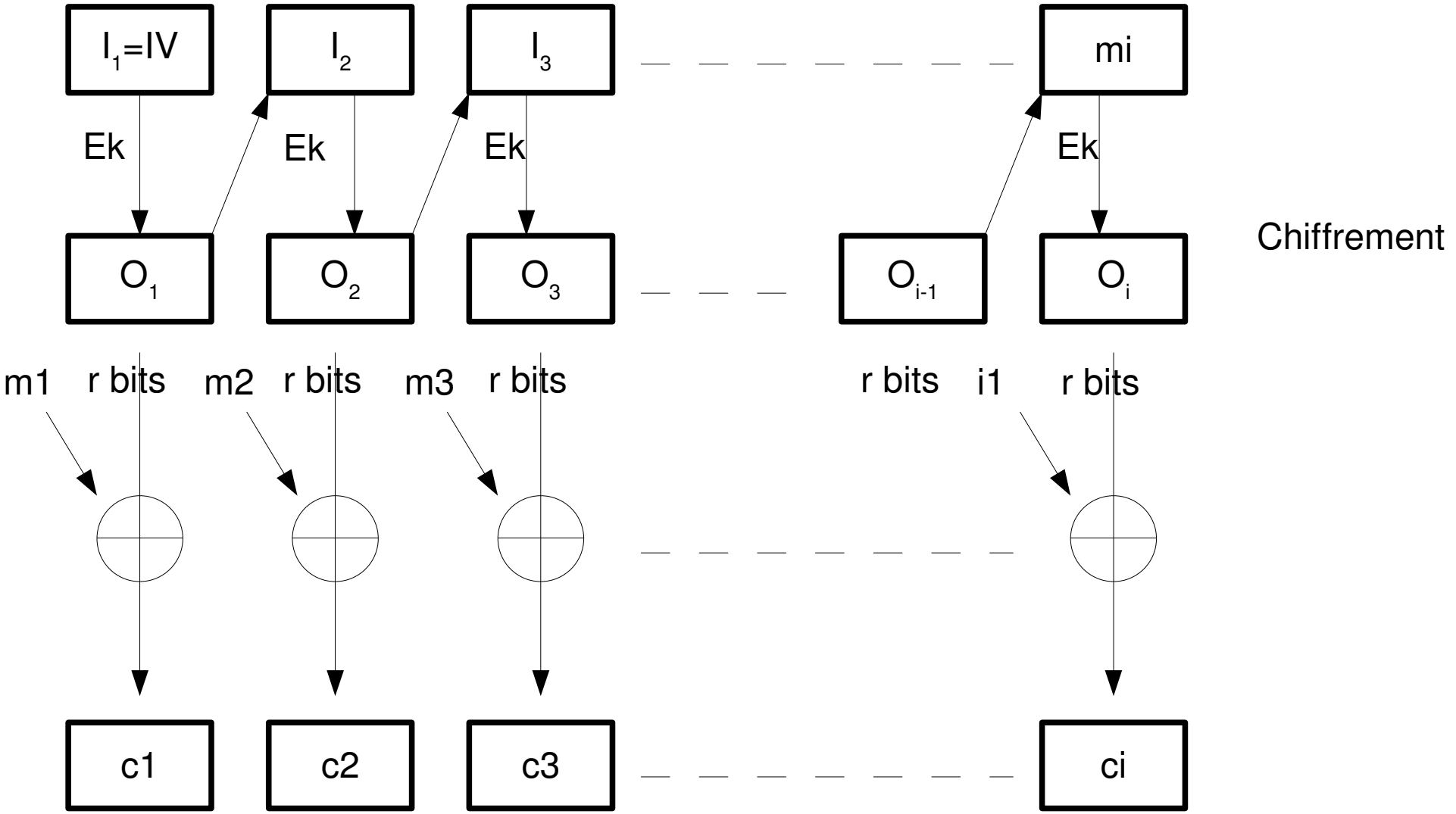
O_j=E(I_j,k)

t_j les r premiers bits de O_j

m_j= $c_j \oplus t_j$

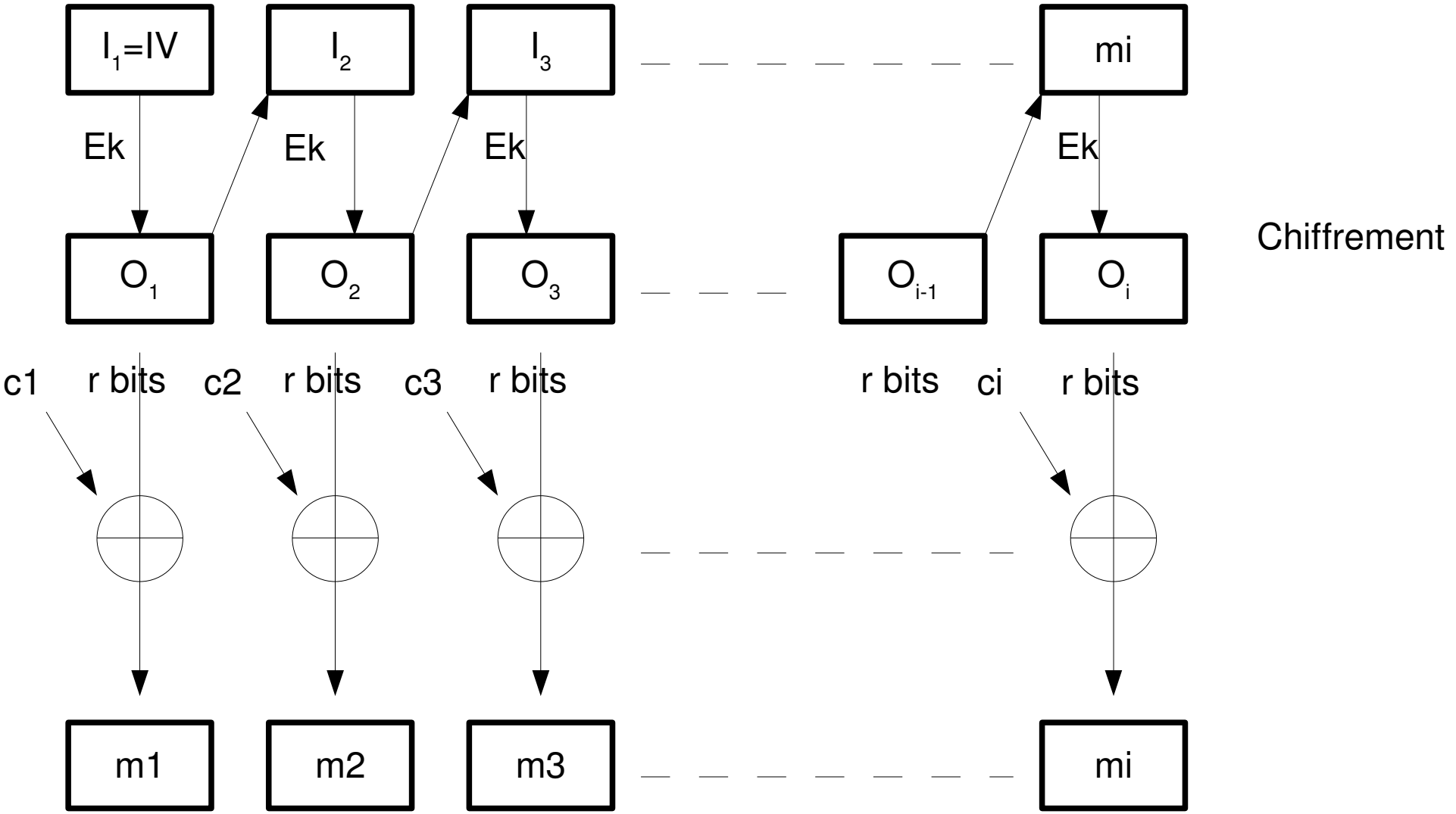
I_{j+1}=O_j

Chiffrement par bloc: OFB



Chiffrement

Déchiffrement par bloc: OFB



Même algorithme que pour le chiffrement

Chiffrement par bloc: OFB

- Avantages:
  - Simplicité
  - Dès qu'on a l'IV, on peut précalculer les O_j ce qui peut être pratique d'un point de vue performances dans certains contextes
  - Deux blocs identiques d'un même fichier seront chiffrés de façon différentes
  - En cas d'erreur, seul le bit erroné sera faux
- Défauts:
  - Le chiffrement d'un bloc en clair dépend seulement de sa position ce qui est plus faible qu'avec cbc où il dépendait du bloc chiffré précédent

Résistance aux erreurs de transmission

- Si un bloc chiffré est détérioré lors des transmissions (un méfait habituel du troll des réseaux), on montrera en TD que :
  - Méthode ECB: Un bloc déchiffré sera verollé
  - Méthode CBC: deux blocs déchiffrés seront verollés
  - Méthode OFB: Un bloc déchiffré sera verollé

Chiffrement par bloc: taille des blocs

- Paradoxe des anniversaires (Richard von Mises):
  - Combien de personnes doit-on rassembler pour avoir plus d'une chance sur deux que deux personnes de ce groupe aient leur anniversaire le même jour de l'année.
  - Réponse: 23, ce qui choque un peu l'intuition.
  - À partir d'un groupe de 57 personnes, la probabilité est supérieure à 99 %

Chiffrement par bloc: taille des blocs

- Produire des blocs chiffrés identiques ouvre la porte à certaines attaques
- Avec des blocs de 64 bits, il faut 2^{32} (# 32Go) blocs distincts pour trouver une collision avec une chance sur deux
  - De nos jours, c'est trop peu
  - Si le mode opératoire est faible (mauvais aléa), la quantité nécessaire peut baisser
- AES utilise des blocs de 128 bits
  - Il faut alors 2^{64} blocs distincts, soit 256 exaoctets pour avoir une chance sur deux de trouver une collision