ircam Centre Pompidou

UPMC SORBONNE UNIVERSITÉS

Bases de l'Arithmétique & Cryptologie Romantique

Ninon Devis: ninon.devis@ircam.fr

TD4

Exercice 11 – Inversion modulaire

6. Déduire de la question précédente un moyen de reconnaître une matrice inversible. Donner alors une nouvelle spécification du chiffrement de Hill, exhiber un exemple de chiffrement et déchiffrement pour une clé bien choisie.

➔ On vient de voir que A est inversible ⇔ $\det A \neq 0$

➔ Pour le chiffrement de Hill: On chiffre successivement des blocs de 2 caractères selon une matrice inversible modulo 7 de taille 2×2 en multipliant chaque bloc de 2 caractères par cette matrice.

➔ Exemple: soit la matrice $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ avec $\det(A) = 2 \times 2 - 3 \times 1 = 1 \neq 0$.

A est inversible mod 7.

On chiffre le mot '123456': on le découpe en blocs représentés par des vecteurs:

$V_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ $V_2 = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ $V_3 = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$ et on multiplie chacun des vecteurs par A:

$V_1 \times A = \begin{pmatrix} 1 \\ 5 \end{pmatrix} \bmod 7$ $V_2 \times A = \begin{pmatrix} 4 \\ 4 \end{pmatrix} \bmod 7$ $V_3 \times A = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \bmod 7$

Donc le chiffré de '123456' est 154403.

Exercice 12 – Cryptanalyse du Chiffrement de Hill

1. Rappelez quelles sont les hypothèses faites lors d'une cryptanalyse à clair/chiffré connu.

➔ On a accès à un couple de clair/chiffré, avec le cryptosystème en boîte noire.

➔ L'accès à cette boîte noire peut être limité ou pas.

➔ On cherche la clef secrète.

2. Supposons la taille m × m de la matrice clef connue. Montrer comment le chiffrement de Hill peut être cryptanalysé à l'aide d'un texte (succession de blocs) clair/chiffré bien choisi.

➔ Soit C la matrice de chiffrés, M la matrice clef, P la matrice des clairs (sous la forme de colonnes) avec P inversible. Pour trouver M la clef, il suffit de résoudre:

$C = MP \iff CP^{-1} = M$ pour trouver la clef M.

Exercice 12 – Cryptanalyse du Chiffrement de Hill

3. Supposons que le texte FRIDAY est chiffré en utilisant le cryptosystème de Hill (modulo 26) avec une taille de blocs m = 2 en le texte PQCFKU. Trouver la clef M.

➔ FR: PQ ID: CF AY: KU

➔ Soit numériquement: (*Rappel: MP = C*)

$$M \times \begin{pmatrix} 5 \\ 17 \end{pmatrix} = \begin{pmatrix} 15 \\ 16 \end{pmatrix} \qquad M \times \begin{pmatrix} 8 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix} \qquad M \times \begin{pmatrix} 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$$

➔ Ce qu'on peut écrire aussi:

$$M \times \begin{pmatrix} 5 & 8 & 0 \\ 17 & 3 & 24 \end{pmatrix} = \begin{pmatrix} 15 & 2 & 10 \\ 16 & 5 & 20 \end{pmatrix}$$

$$M \times P^* = C^*$$

➔ Pour déchiffrer le message, il suffit qu'une matrice carrée formée avec deux des trois colonnes présentes dans P*, ait un déterminant premier avec n = 26.

Exercice 12 – Cryptanalyse du Chiffrement de Hill

➔ Essayons avec les deux premières colonnes de P*: $P^* = \begin{pmatrix} 5 & 0 & 0 \\ 8 & 3 & 24 \end{pmatrix}$

$P = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$

det(P) = $5 \times 3 - 17 \times 8 = -121 = 9 \mod 26$.

$P^{-1} = \frac{1}{\det P}\, {}^{t}\mathrm{com}\, P$

Rappels: deux entiers *a* et *n* sont premiers entre eux, on sait qu'il existe deux nombres *u* et *v* tels que *au* + *nv* = 1. Modulo *n*, cette égalité devient *au* = 1 (mod *n*).

Autrement dit, si *a* et *n* sont premiers entre eux, alors *a* possède un « inverse » u modulo *n*.

➔ $9 \times 3 = 1 \mod 26$

Exercice 12 – Cryptanalyse du Chiffrement de Hill

$C^* = \begin{pmatrix} 15 & 2 & 10 \\ 16 & 5 & 20 \end{pmatrix}$

➔ On résout donc modulo 26 le système:

- $M = CP^{-1} = \begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}^{-1}$
- Rappels: $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $A^{-1} = \frac{1}{\det A} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
- D'où: $P^{-1} = \frac{1}{\det P} \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix}$ avec $9 \times 3 = 1 \mod 26$

soit: $P^{-1} = \frac{1}{\det P} \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = 3 \times \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$

Exercice 12 – Cryptanalyse du Chiffrement de Hill

➔ On calcule donc:

$M = CP^{-1} = \begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix}\begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$

➔ On vérifie sur la troisième colonne:

Rappels: $M \times \begin{pmatrix} 5 & 8 & \boxed{0} \\ 17 & 3 & \boxed{24} \end{pmatrix} = \begin{pmatrix} 15 & 2 & \boxed{10} \\ 16 & 5 & \boxed{20} \end{pmatrix}$

$\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}\begin{pmatrix} 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$

➔ D’où on a bien trouvé la clef M = $\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$.

Exercice 13 – Vigenère par mot probable

On s'intéresse ici à une méthode de cryptanalyse générale, celle du mot probable, appliquée au chiffrement de Vigenère. Dans tout cet exercice on part donc de l'hypothèse que nous connaissons un mot probable dans le texte clair et que le cryptosystème utilisé est de type Vigenère.

1. Expliquez comment vous pourrez utiliser cette hypothèse pour cryptanalyser un texte chiffré. Vous décrirez bien toutes les hypothèses nécessaires pour mener à bien votre cryptanalyse.

➔ Hypothèses pour la cryptanalyse:

- sur le mot probable, il nous faut connaître: la position -
- sur la clef: longueur ≤ longueur du mot probable.

➔ Dans ce cas, on fait l'hypothèse que le mot probable se trouve dans la 1ère colonne So et on en déduit do la décalage de cette colonne -

Exercice 13 – Vigenère par mot probable

2. Vous avez intercepté un message hier à destination d'un sous-marin ennemi (francophone). Sachant que ces messages commencent toujours par un bulletin météo de la forme lundi ciel bleu etc. ou encore vendredi orage venant de l'ouest etc. et que le mot clé est rarement de longueur plus grande que 5. On vous demande de cryptanalyser cette interception.

```
YURGQ ZOAJM EYTDD QLSHA MNTDY GYSXZ XCLHX MLLHA F
```

- Tous les jours de la semaine ont au moins: 5 lettres
- Donc on cherche une clef de longueur: 5

- Sachant que lundi ne donne pas un texte intelligible, essayer avec mardi!
  TODO

Exercice 14 – Vigenère et échange de clef

Chiffrements de Vigenère à l'aide de clés de longueur identique fixée l. Les chiffrements sont tous des applications de A^l dans A^l et peuvent être rassemblés dans un l'ensemble: $V^l = \{e_K : A^l \to A^l \mid e_K$ un chiffrement de Vigenère de clé K de longueur l$\}$

1. On veut munir l'ensemble V^l de l'opération de composition dénotée ◦ Montrer que V^l est stable par composition. => pour tout couple d'élément de V^l la composition est possible et elle résulte en un élément de V^l.

$\forall m_1 \dots m_l \in V^l : e_{K1} \circ e_{K2}(m_1, \dots m_l) = e_{K1}(e_{K2}(m_1, \dots, m_l)$

$= e_{K1}((m_1 + K_{2_1}) \bmod 26 \dots (m_l + K_{2_l}) \bmod 26)$

$= (((m_1 + K_{2_1}) \bmod 26 + K_{1_1}) \bmod 26 \dots (((m_l + K_{2_l}) \bmod 26) + K_{1_l}) \bmod 26$

$= (m_1 + (K_{2_1} + K_{1_1}) \bmod 26) \bmod 26 \dots (m_l + (K_{2_l} + K_{1_l}) \bmod 26) \bmod 26$

d'où $e_{K1} \circ e_{K2} = e_{K3}$ avec $K_{3i} = K_{1_i} + K_{2_i} \bmod 26$

Exercice 14 – Vigenère et échange de clef

2. Montrer que l'ensemble V^l muni de la composition forme un groupe. Montrer de plus qu'il est commutatif. $(V^l, +, 0)$

- L'addition sur les entiers modulo 26 est commutative et associative
  - dotée de l'élément neutre 0
- Tout élément x, a pour opposé $26 - x$
- La composition sur V^l est stable, commutative et associative
  - a pour élément neutre la clef $0, \dots, 0$
  - l'opposé d'une clef $k_1 \dots k_l$ est $(26 - k_1) \dots (26 - k_l)$

➔ Donc V^l muni de la composition forme un groupe commutatif.

Exercice 14 – Vigenère et échange de clef

Chiffrement de Vigenère pour réaliser un échange de clé sans rencontre préalable. Alice initialise et choisit donc la clé K. Alice et Bob se sont mis d'accord et n'utilisent que des fonctions de chiffrement issues de V^l .

1 : Alice choisit une clé K_1 aléatoire de longueur l et envoie $s_1 = e_{K1}(K)$ à Bob

2 : en retour, Bob choisit une clé K_2 aléatoire de longueur l et envoie $s_2 = e_{K2}(s_1)$ à Alice

3 : finalement Alice réalise un dernier envoi à Bob.

3. Expliquer quel est le dernier envoi réalisé par Alice pour être sûr que Bob ait en sa possession la clé K.

Alice envoie: $s_3 = e_{K1}^{-1}(s_2) = e_{K1}^{-1}(e_{K2}(s_1)) = e_{K1}^{-1}(e_{K2}(e_{K1}(K)))$

$= e_{K2}(e_{K1}^{-1}(e_{K1}(K))) = e_{K2}(K)$ –

Bob calcule alors: ⟶

$e_{K2}^{-1}(s_3) = K$ –

Exercice 14 – Vigenère et échange de clef

4. Montrer qu'un attaquant peut retrouver la clé K très facilement à partir de s_1, s_2 et le troisième envoi d'Alice.

De s_1 et s_2 on a: $s_2 = e_{K_2}(s_1)$. On peut en déduire K_2 caractère par caractère - car: $K_{2,i} = (s_{2,i} - s_{1,i}) \bmod 26$ c'est à dire: $K_2 = e_{s_1}^{-1}(s_2)$

➔ On dispose de la même information que Bob et comme lui on peut déduire de la valeur de K en recevant le dernier message.

➔ Il est possible de faire le même raisonnement avec n'importe quel couple de message.

Exercice 14 – Vigenère et échange de clef

5. Quelles propriétés doit vérifier un chiffrement symétrique pour que l'on puisse l'utiliser en remplacement du chiffrement de Vigenère dans le cadre d'un échange de clé en trois passes comme expliqué précédemment ?

Il faut que la connaissance d'un message clair et du chiffré correspondant ne dévoile pas la clef utilisée dont on pourrait se servir pour s_3 ou s_2.

6. Rappeler l'avantage spécifique au chiffrement One-time Pad de Vernam. Pourrait-il convenir dans le cadre de la question précédente ?

- Chiffrement parfait et incassable.
- Rappels: chiffrement de Vernam = chiffrement de Vigenère avec une clef de longueur la longueur du message à transmettre.

	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	message (HELLO)
+	22 (W)	12 (M)	2 (C)	10 (K)	11 (L)	masque (WMCKL)
=	29	16	13	21	25	masque + message
=	3 (D)	16 (Q)	13 (N)	21 (V)	25 (Z)	masque + message modulo 26

Exercice 14 – Vigenère et échange de clef

6. Rappeler l'avantage spécifique au chiffrement One-time Pad de Vernam. Pourrait-il convenir dans le cadre de la question précédente ?

- Même défaut que que le chiffrement précédent puisque c'est un chiffrement de Vigenère.
- On utilise K_1 deux fois donc on casse le principe du One-Time-Pad.

7. L'indicateur dépose dans un lieu anonyme un message chiffré avec l'explication du procédé de chiffrement utilisé et prévient le policier de l'endroit où il peut retrouver les données de l'indicateur. Montrer comment ils peuvent procéder pour que l'échange de données se fasse de manière anonyme.

Soit m la donnée à transmettre. L'indicateur dépose $s_1 = e_{k_1}(m)$

Le policier dépose ensuite: $s_2 = e_{k_2}(s_1)$

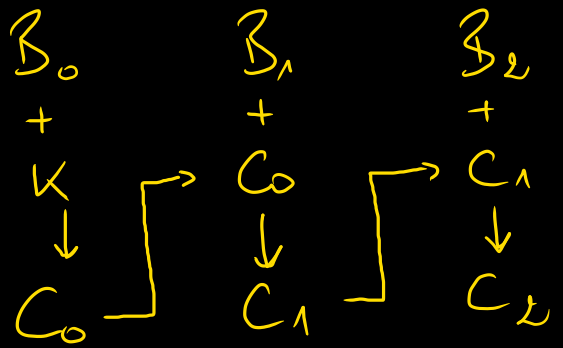
L'indicateur dépose: $s_3 = e_{k_1}^{-1}(s_2)$

Le policier obtient m = $m = e_{k_2}^{-1}(s_3)$

Exercice 15 – Vigenère autoclave

On s'intéresse ici à une utilisation du cryptosystème de Vigenère avec une clé de longueur m pour chiffrer un texte de plusieurs blocs de longueur m chacun. Pour chiffrer le premier bloc B_0 du texte on utilise le chiffrement de Vigenère avec la clé privée K. Pour un bloc B_i arrivant à la position $i > 0$ dans le texte, on utilise le chiffrement de Vigenère en prenant comme clé le chiffré du bloc B_{i-1}.

1. Représenter le chiffrement d'un texte de n blocs de longueur m à l'aide d'un schéma. Expliquer comment déchiffrer ce texte. $m = B_0 \| B_1 \| B_2 \dots$



Pour le chiffrement:

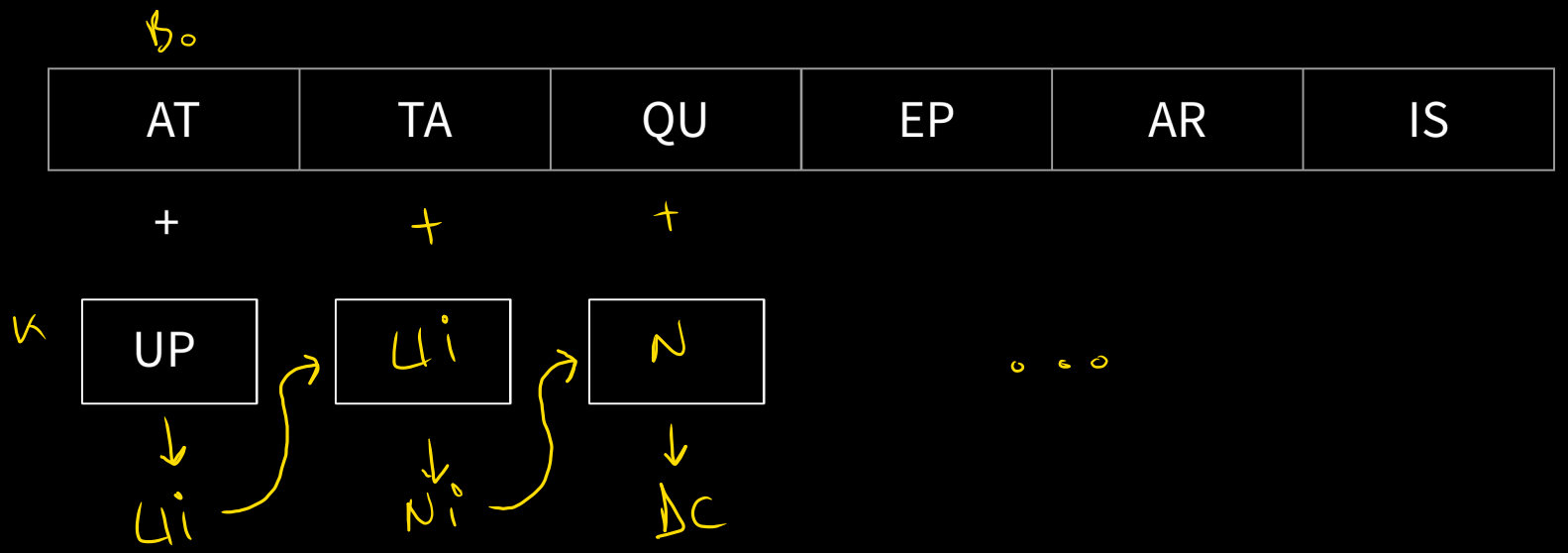
$C_0 = e_K(B_0)$ $C_{i+1} = e_{C_i}(B_{i+1})$

Pour le déchiffrement:

$B_0 = e_K^{-1}(C_0)$ $B_{i+1} = e^{-1}_{C_i}(C_{i+1})$

Exercice 15 – Vigenère autoclave

2. À l'aide de ce cryptosystème, chiffrer le texte ATTAQUEPARIS avec la clé K =UP.

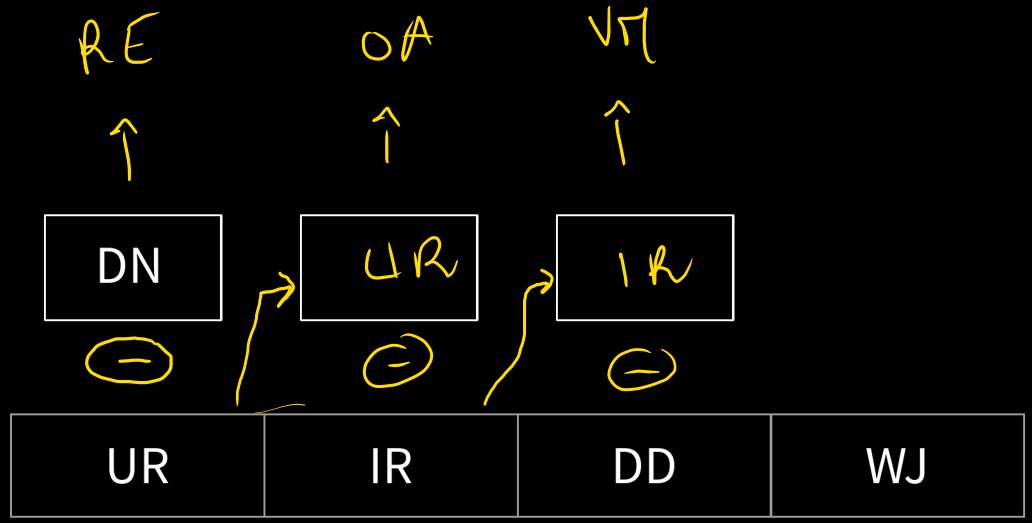


A = 0, avec la clef U = 20, 0 + 20 = 20 => A devient U.

T = 19, avec la clef P = 15, 19 + 15 = 34 = 8 mod 26 => T devient I.

Exercice 15 – Vigenère autoclave

2. Déchiffrer le texte URIRDDWJ avec la clé DN.



U = 20, avec la clef D = 3, 20 - 3 = 17 => U devient R.
R = 17, avec la clef N = 13, 17 - 13 = 4 => R devient E.

Exercice 15 – Vigenère autoclave

3. Supposons que la longueur de la clé soit connue. Est-ce que l'utilisation du cryptosystème de Vigenère de cette manière peut être cryptanalysée avec les techniques vues en cours/TD/TME ? Si non, est-il pour autant plus sûr que l'utilisation classique de Vigenère ? (Argumentez vos réponses.)

- Techniques vues en cours: ne fonctionnent pas car elles permettent de chercher une clef qui chiffre tout le texte.
- Ici la protection se trouve sur le 1er bloc

- Si on connaît la longueur de la clef, on déchiffre tout le texte sauf le premier bloc avec ce chiffrement.

Exercice 16 – Cryptanalyse de Vigenère

1. Un texte a été chiffré en utilisant le chiffrement de Vigenère avec une clé de taille l. Donner les entiers les plus probables pour la longueur de la clé l. Vous expliquerez votre démarche.

- Indice de coïncidence: très long !
- Test le plus judicieux: Kasiski !

HIBKA	UQFLF	SBQSX	SKCFB	YOAGP	ALGTC	RTYTL
DGBYO	AGPAL	OAKYB	FBILY	OYQTD	ISVAI	JJNNA
DXNLW	NRQPF	BVPWN	IWAFB	YAANR	URTZE	LYZLF
MEWHI	BKAUQ	FLALJ	GTXRG	VNIJP	ZREQL	KWZA

→ fastidieux

HIBKA : [0, 108]

YOAGPAL : [19; 37]

écart de 108 et 18 –

La longueur de la clef est donc probablement un multiple de 18

(9) / 18

↳ d'après les exos précédents –