CAHIERS AFRICAINS DES DROITS DE L'HOMME ET DE LA DÉMOCRATIE AINSI QUE DU DÉVELOPPEMENT DURABLE
REVUE AFRICAINE INTERDISCIPLINAIRE

ISSN : 2791-1063 (Imprimé)
ISSN : 2791-1071 (En ligne)

27ème année - Numéro 78 - Volume 1 - Janvier-Mars 2023

UN NOUVEAU SYSTÈME DE CHIFFREMENT DE DONNÉES HYBRIDE BASÉ SUR LE CALCUL MATRICIEL DANS L'ANNEAU MODULAIRE DANS Z_{79}

Par

Joël KINGANGA MAKANGA
Chef de Travaux, à la Mention Mathématiques, Statistique et Informatique, Université de Kinshasa, Faculté des Sciences et Technologie, Kinshasa/RDC

Nathanaël KASORO MULENDA
Professeur Ordinaire, à la Mention Mathématiques, Statistique et Informatique, Université de Kinshasa, Faculté des Sciences et Technologie, Kinshasa/RDC

Alain MUSESA LANDA
Professeur Ordinaire, à la Mention Mathématiques, Statistique et Informatique, Faculté des Sciences et Technologie, Université de Kinshasa, Kinshasa/RDC

RÉSUMÉ

La sécurité des données reste l'un des domaines de recherche exploités par les chercheurs aujourd'hui, notamment en raison de l'émergence d'Internet, qui génère chaque jour de grandes masses de données. Actuellement, pour garantir la confidentialité des données, plusieurs systèmes cryptographiques basés sur le calcul matriciel utilisent le chiffrement bigraphique (matrices carrées d'ordre 2) avec l'alphabet normal modulo 26, c'est le cas pour chiffrement de Hill. Cependant, cette méthode de cryptage n'est pas sûre et fiable à cause de la linéarité de sa combinaison. L'objectif de cet article est de proposer un système de cryptage hybride utilisant une matrice carré de grande taille, afin de garantir une meilleure confidentialité des données, ce nouveau système ajouté à la vitesse de cryptage symétrique avec le calcul matriciel, la force de cryptage asymétrique proposée par RSA (Riverst, Shamir, and Adleman). Les résultats obtenus et la complexité de la nouvelle méthode montrent la fiabilité et la robustesse du système hybride proposé.

Mots-clés : *Cryptage, Décryptage, Matrice, RSA, Symétrique, Asymétrique, Hybride, système, Alphabet, Algorithme.*

ABSTRACT

Data security remains one of the research areas being exploited by researchers today, particularly due to the emergence of the Internet, which generates large masses of data every day. Currently, to guarantee the confidentiality of data, several cryptographic systems based on matrix compitation use bigraphic encryption (square matrices of order 2) with the normal alphabet mod 26, which is the case for Hill encryption.

However, this encryption method is not secure and reliable because of the linearity of its combination. The objective of this paper is to propose a hybrid encryption system using a large square matrix, in order to guarantee a better confidentiality of data, this new system added to the symmetric encryption speed with the matrix calculation, the asymmetric encryption strength proposed by RSA (Riverst, Shamir, and Adleman). The results obtained and the complexity of the new method show the reliability and robustness of the proposed hybrid system.

Keywords: *Encryption, Decryption, Matrix, RSA, Symmetric, Asymmetric, Hybrid, System, Alphabet, Algorithm*

INTRODUCTION

La cryptographie est devenue un véritable enjeu de société au cours des dernières décennies, suite au développement rapide des technologies de l'information et de la communication ainsi que des infrastructures de réseaux filaires et sans fil. Plusieurs chercheurs ont montré que l'augmentation du nombre d'utilisateurs, ainsi que le développement rapide des réseaux de communication numérique, ont fait de la sécurité des données un problème critique. [Historiquement développé pour assurer le secret de la messagerie, le cryptage de l'information est maintenant utilisé plus largement pour empêcher l'accès ou la modification d'informations sensibles et pour assurer la confidentialité dans les applications informatiques[1]. Les caractères sont cryptés et décryptés à l'aide d'algorithmes ainsi que de clés de cryptage.

L'objectif fondamental de la cryptographie est de permettre à deux personnes de communiquer par un canal non sécurisé de telle sorte qu'un adversaire, qui a accès aux informations circulant sur le canal de communication, ne puisse pas comprendre ce qui est échangé. Le canal peut être, par exemple, une ligne téléphonique ou tout autre réseau de communication[2].

Plusieurs techniques de cryptage ont été développées ces dernières années. Malheureusement, dans la plupart de ces techniques, les auteurs utilisent des matrices carrées du second ordre en mode EBC avec l'alphabet normal pour chiffrer les données. Ces techniques présentent quelques inconvénients, entre autres l'attaque par force brute, car la taille de la matrice est trop petite. Le temps d'exécution est trop long car les caractères sont des nombres deux par

[1] P. Kuppuswamy, S. Q. Yahya Al Khalidi Al-Maliki, "A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm", *Bulletin of Electrical engineering and Informatics*. Vol. 12, No 2, pp. 1448-1458, DOI: https://doi.org/10.11591/eei.v12i2.4967

[2] J.G. DUMAS, *Théorie des codes Compression, Cryptage, Correction*, édition Dunod, Paris, 2007. pp.145.

deux, des prix parmi les 26 lettres de l'alphabet, et d'autres caractères comme les caractères spéciaux ne sont pas pris en compte. Une fois reconnu après son chiffrement, un caractère révèle peu les informations du cache.

Plusieurs études ont fait l'objet de chiffrement ce dernier temps. D'autres auteurs parlent de la protection des bases de données en effectuant des comparaisons rapides pour deux chiffrements, c'est-à-dire des comparaisons où il n'est pas nécessaire de décrypter complètement les deux chiffrements comparés[3]. D'autres aussi parlent d'une nouvelle méthode pour analyser et optimiser les générateurs thermoacoustiques pour la récupération de l'énergie résiduelle[4]. D'autres auteurs démontrent le cryptage d'images médicales basé sur des cartes chaotiques. Dans ce travail, les auteurs trouvent un système de cryptage d'images médicales basé sur un générateur de clés utilisant le mélange de cartes chaotiques et une technique de confusion-diffusion de données[5]. Ils implémentent un algorithme avec trois cartes chaotiques, Logistique, Chebyshev et la carte standard.

Dans ces articles, nous proposons un système de chiffrement hybride basé sur les matrices mode de cryptage CBC et un alphabet désordonné qui inclut tous les caractères, y compris les caractères dits spéciaux, et empêche les attaques par force brute[6].

Hormis cette introduction, Ce document est structuré comme suit : la première section présente les concepts clés entourant le thème de la recherche. Dans la deuxième section, nous abordons les matériels et les méthodes utilisés dans cette recherche. Dans la troisième section, nous présentons le système hybride proposé. La dernière section explique un exemple d'application de cette nouvelle méthode avant de conclure et de présenter les perspectives de notre recherche.

---

[3] S. JACOB. Thèse de doctorat : " *Protection cryptographique des bases de données : Conception et cryptanalyse. Cryptographie et sécurité* ". Université Pierre et Marie Curie - Paris VI, 2012. Français.

[4] C. INIESTA, et Al. "New method to analyse and optimise thermoacoustic power generators for the recovery of residual energy", *Alexandria Eng. J.* , vol. 59, no. 5, pp. 3907-3917, oct. 2020, doi : 10.1016/j.aej.2020.06.046.

[5] S. PATEL, K. Bharath , et M. Rajesh Kumar, "Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique," *Multimed. Tools Appl.* vol. 79, no. 43-44, pp. 31739-31757, Nov. 2020, doi : 10.1007/s11042-020-09551-9

[6] S. Nagaraj, P. Raju & Kishore Bhamidipati. "A New Substitution Block Cipher Using Genetic Algorithm". *Conference on Frontiers of Intelligent Computing: Theory and Applications*. pp 339–347. DOI: 10.1007/978-3-642-35314-7_39.

I. CONCEPTS CLÉS

Dans cette section, nous définissons certains concepts nécessaires à la compréhension de notre sujet de recherche.

I.1. Cryptographie

La cryptographie est l'une des premières propositions visant à assurer la transmission et le transfert sécurisés de documents sur le Net. La cryptographie est une technique largement utilisée pour protéger le contenu numérique des médias. Le message est crypté avant la transmission et décrypté à l'extrémité réceptrice à l'aide d'une clé, de sorte que personne ne puisse accéder au contenu sans disposer de la véritable clé. Le message est appelé le texte et le message crypté est appelé le texte chiffré. L'information est protégée avant le moment de la transmission, mais après le décryptage, l'information devient non protégée et peut être copiée et distribuée[7].

I.2. Cryptanalyse

La cryptanalyse vise à analyser les méthodes proposées par la cryptographie afin de trouver les clés secrètes utilisées ou, à défaut, de pouvoir retrouver un texte clair à partir d'un texte chiffré. Il existe deux types de cryptanalyse : la cryptanalyse mathématique et la cryptanalyse physique. La cryptanalyse mathématique étudie la solidité des algorithmes en se concentrant sur leurs propriétés mathématiques. Cette partie a été la première à être explorée et développée. La cryptanalyse dite physique, quant à elle, étudie plus particulièrement les faiblesses liées aux composants sur lesquels les algorithmes cryptographiques sont implémentés[8].

I.3. Cryptage, décryptage

L'idée de base du cryptage est de modifier le message de telle sorte que seul l'utilisateur légal puisse en reconstituer le contenu. En d'autres termes, le chiffrement est un procédé cryptographique par lequel on veut rendre impossible la compréhension d'un document par quiconque ne disposant pas la clé de déchiffrement. L'objectif du cryptage des données est de protéger la confidentialité des données numériques lorsqu'elles sont stockées et transmises via un support de communication. Le décryptage est l'opération inverse[9].

I.4. Encodé, décodé

L'encodage consiste à encapsuler un ensemble d'informations avec une clé, et cet ensemble d'informations ne peut sortir de la capsule qu'à l'aide d'une clé (qui peut être différente de la clé d'encodage). On parle alors de décodage.

---

[7] D. Courant: "From kleroterion to cryptology: The act of sortition in the twenty-first century — instruments and practices", *cairn info International Edition*, pp 343-372, 2019.

[8] Idem.

[9] M. Madani: "Medical image encryption based on chaotic maps". *Computers in Biology and Medicine* , vol. 43, pp. 1000-1010, 2015.

II. MATÉRIELS ET MÉTHODES

II.1. Matériels

La mise en œuvre concrète du système hybride proposé a nécessité l'utilisation de certains matériels. Le langage Python a été utilisé pour le codage du nouvel algorithme proposé. L'outil MathLab a été d'une importance capitale dans le sens où il nous a permis de montrer graphiquement les résultats obtenus dans notre recherche.

II.2. Méthodes

II.2.1. Les chiffres de Hill

Le chiffre de Hill fait partie des cryptages asymétriques qui utilisent des matrices carrées du second ordre pour le cryptage des données.[10] Pour les rendre encore plus compliqués, les auteurs proposent de permuter les lettres avant de les chiffrer à l'aide des algorithmes, ce qui est nécessaire au début, puis d'augmenter la taille de la matrice de chiffrement. Au lieu d'utiliser des matrices d'ordre 2 comme le faisait le mathématicien Hill à l'époque, opter pour des matrices inversibles d'ordre 4, 5 ou même 10 serait mieux et enfin modifier les nombres associés aux lettres, c'est-à-dire surcrypter les chiffres[11]. Au lieu de prendre A = 1, B=2, C=3 et ainsi de suite, il est préférable de prendre par exemple A=24, B=19, C=3, D= 11.

II.2.2. RSA

En 1977, trois mathématiciens américains, Ronald Rivest, Adi Shamir et Leonard Adleman, ont mis au point un système asymétrique qui reste le meilleur et le plus utilisé à ce jour : le système RSA (du nom des initiales des trois auteurs). Pour comprendre cet algorithme, supposons, par exemple, que deux personnes souhaitent échanger des messages secrets en ligne[12]. Elles doivent procéder comme suit :

1. Choisissez deux grands nombres premiers p et q. Les deux p et q doivent contenir au moins 150 décimales.
2. Calculer $n = p*q$
3. Choisissez un petit entier e premier avec (φn) = $(p - 1)(q - 1)$
4. Calculer d, l'inverse de e par multiplication modulo '(n).
5. Publier la paire $_{Ke}$ = (e, n) comme sa clé publique RSA.
6. Garder secrète la paire $Kd = (d, n)$ qui est sa clé privée RSA.

[10] S. Kumar, H.T. Panduranga & S.K. Naveen Kumar. "Hybrid Approach for Image Encryption Using Hill Cipher Technique". *Conférence internationale sur le traitement de l'information,* pp 200-205. DOI: 10.1007/978-3-642-31686-9_23.

[11] J. BASAVAIAH, A. Anthony & C. Mohan Patil . "Cryptographie visuelle utilisant le chiffrement de Hill et les techniques avancées de chiffrement de Hill". *Advances in VLSI, Signal Processing, Power Electronics, IoT, Communication and Embedded Systems* pp 429-443. DOI: 10.1007/978-981-16-0443-0_34

[12] V. DOMINUS : La cryptographie Asymétrique avec RSA. Août 2019, pp. 3.

Nous avons alors :

- Cryptage RSA : $E(M) = M^e \pmod{n}$
- Décryptage RSA : $D(M) = M^d \pmod{n}$

III. SYSTÈME HYBRIDE PROPOSÉ

Puisque la cryptographie asymétrique est basée sur des problèmes mathématiques complexes (factorisation de grands entiers ou équation du logarithme discret). L'utilisation du système cryptographique RSA serait un bon choix car il est basé sur le principe de deux clés : la clé publique et la clé privée. La clé publique est mise à la disposition de toute personne souhaitant chiffrer un message (cette clé peut être connue de tous). Le message ne peut être décrypté qu'avec la clé privée, qui doit être confidentielle et connue uniquement de son propriétaire. Le cryptosystème hybride proposé utilise les avantages du cryptage symétrique et asymétrique, qui sont la rapidité et la possibilité de ne pas transmettre la clé secrète à travers un cryptosystème.

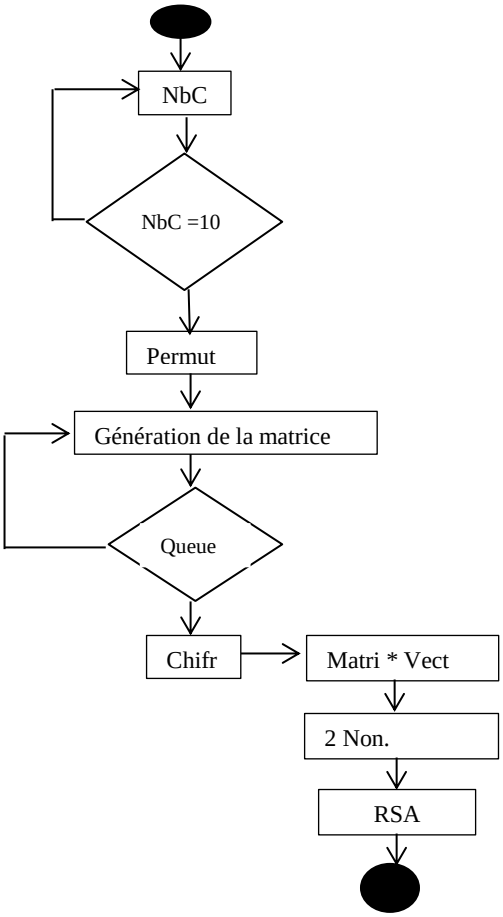

Fig.1 : Diagramme de l'étape de cryptage

Comme le montre le diagramme ci-dessus, les données à crypter doivent être en blocs de 10 pour éviter le décryptage par la méthode du texte par force brute et permutées avant le cryptage à l'aide d'un algorithme de cryptage. Nous avons généré une matrice carrée dont la taille est le nombre de blocs de caractères de cryptage. Dans notre cas, il s'agit de la taille 10. La figure 2 illustre cette approche.

III.1. Phase 1 : Permutation de données

Comme mentionné ci-dessus, nous avons utilisé un algorithme de permutation de caractères (Figure 2). Ce dernier permet de permuter l'ordre des caractères du message à crypter pour rendre l'attaque par force brute difficile avant même le cryptage.

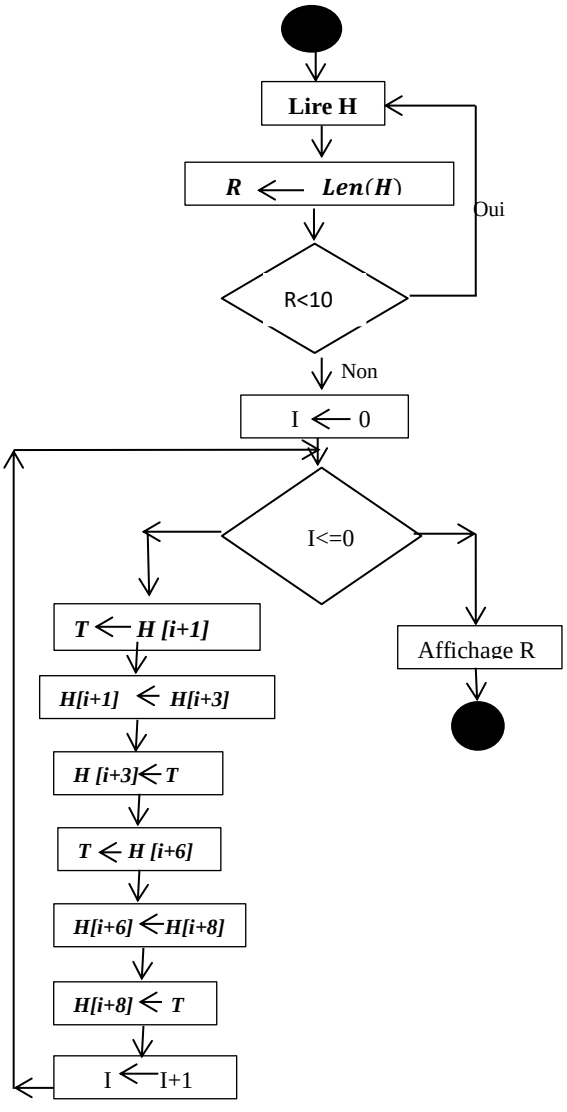

Fig. 2 : Diagramme de permutation des caractères

III.2. Phase 2 : Correspondance des caractères dans l'alphabet désordonné

Après avoir permuté les caractères, notre nouveau système utilise l'alphabet désordonné, c'est-à-dire qu'au lieu de dire que A= 1, B=2, ...Y=25, le système remplace chaque lettre par son ordre dans l'alphabet désordonné ; A=17, B=9, C=21, D=2, E=13 et ainsi de suite. Pour ce cryptage, en plus des lettres alphabétiques, le système utilisé également des caractères spéciaux tels que \#, @, \&, /, ! Cela signifie que l'ensemble des caractères utilisés pour le cryptage est supérieur à 26. Donc 79 pour notre cas.

Pour cela, le texte chiffré doit être remplacé par une valeur numérique en fonction de son rang dans l'alphabet désordonné. Ces valeurs seront considérées comme une matrice vectorielle de rangs 10, identique à la taille de notre matrice. L'algorithme de correspondance des caractères se présente comme suit :

Algorithme 1 *: Algorithme de mise en correspondance*
Entrée(s) *: Une liste H contenant les caractères composer une phrase ou un mot*
Sortie(s) *: Une liste N contenant les nombres correspondant*

```
N= [ ]
Pour i dans H
    Si i= "a" ou i= "A
        AA=12
        N=AA
    Sinon Si i= "b" ou i= "B
        BB=27
        N=BB
    Sinon Si i= "c" ou i= "C
        CC=16
    .....
    Sinon Si i= " / "
        Joe2=24
        N=joe2
    Sinon Si i= "@"
        joe3=35
        N=joe3
    Fin si
Fin
```

III.3. Phase 3 : Générer une matrice carrée d'ordre 10

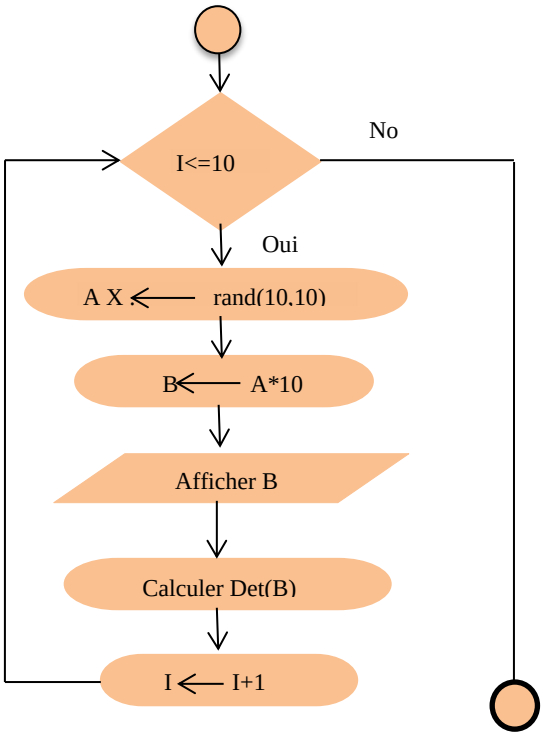

Fig.3. Diagramme du générateur de matrice carrée.

La troisième phase de notre Algorithme consiste à générer une matrice carrée d'ordre 10 pour le cryptage. L'ordre de la matrice à générer doit correspondre au nombre de caractères à crypter. La matrice de cryptage doit être bien choisie. Pour que le processus soit inversible, la matrice doit être inversible dans $Z/_{79Z}$. En d'autres termes, le déterminant de cette matrice doit être positif, non nul, et avoir un inverse dans $Z/_{79Z}$, c'est-à-dire que le déterminant doit être premier avec 79, qui est le nombre total de caractères de cryptage.

Le vecteur trouvé dans l'algorithme de correspondance sera multiplié par la matrice carrée générée pour trouver une autre matrice de vecteur de ligne qui sera chiffrée avec RSA. L'algorithme de génération de matrice est donné dans la figure 3. Soit M la matrice trouvée, et H, le bloc de caractères chiffrés, les caractères L_j et L_{j+1} du message à chiffrer, c'est-à-dire de H, seront chiffrés C_j et C_{j+1} selon cette formule :

$$C_j = M_{ij} * H_j \pmod{79} \quad (1)$$

Avec :

- C_j : Caractères de chiffrement
- M : matrice carrée générée de taille n, avec (n=10)
- H : Matrice contenant les caractères à crypter (C_j)

Les n caractères du message d'un mot ou d'une phrase seront chiffrés selon la formule ci-dessous :

$$C_i = \sum_{ij=1}^{n} M_{ij} * H_i (\text{mod } 79) \quad \textbf{(2)}$$

La phase de cryptage est fermée avec RSA, elle se fait avec la formule :

$$x = M^e (\text{mod } n) \quad \textbf{(3)}$$

Avec :

- *x : message à envoyer au destinataire*
- *M : caractères à crypter (ici M est un nombre entier)*
- *e : la clé publique*
- *n : la clé publique*

La deuxième étape porte sur le décryptage. L'opération de décryptage est le processus inverse du cryptage, sauf que la matrice générée avec notre algorithme de la figure 6 doit être inversible dans $Z/_{79}$. Cela n'est possible que si son déterminant est non nul dans $Z/_{79}$. En d'autres termes, le déterminant de la matrice (M) et 79 doivent être premiers, c'est-à-dire que leur pgcd=1. Quelques étapes suffisent pour effectuer le décryptage. Tout d'abord, trouver le déterminant de la matrice et son inverse en utilisant l'algorithme euclidien, puis trouver la matrice de décryptage en multipliant l'inverse du déterminant avec la matrice générée modulo 79.

*** Diagramme de déchiffrement de données : Bloc Récepteur**

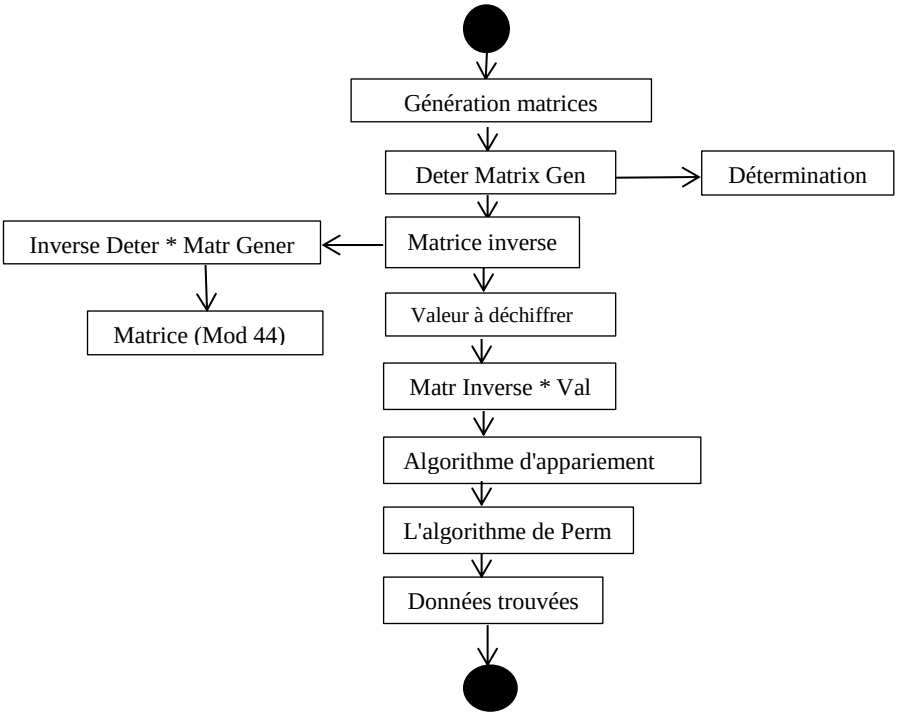

Fig. 4: Schéma de l'étape de décryptage

Pour le décryptage, le processus est le même, mais cette fois ci, le système doit trouver l'inverse de la matrice de départ ou matrice de cryptage. Mais d'abord, le système va utiliser le cryptage RSA pour décrypter le message envoyé. Les valeurs trouvées après le cryptage RSA correspondraient à chaque caractère crypté. Avant de trouver l'inverse de la matrice de départ, le système sera obligés de décrypter avec RSA pour trouver le vecteur ligne. En d'autres termes :

$$y = M^{d} (\mathrm{mod}\, n) \qquad (4)$$

Avec :

- ***y*** *: caractères trouvés après le décryptage RSA*
- *M : tout à déchiffrer*
- *d : la clé privée*
- *n : la clé publique.*

Pour trouver l'inverse de cette matrice, il faut d'abord trouver son déterminant et l'inverse de ce déterminant modulo 79. C'est-à-dire qu'il existe une valeur dans $Z/_{79}$ qui est l'inverse du déterminant et pour s'assurer que cette valeur existe, le PGCD (79, Det) doit être égale à 1. En d'autres termes ; on

calcule l'inverse ***d*** de ***e*** module φ**(*n*) : *d* x *e* ≡ 1 (mod φ(*n*)).** Ce calcul est effectué par l'algorithme d'Euclide étendu**. Le** φ**(*n*) est** calculée.

$$d * e \equiv 1(\mathrm{mod}\,\varphi(n)) \quad (5)$$

- *e : exposant choisi par l'émetteur*
- *d : l'inverse de la recherche qui est aussi la clé privée*
- *φ(n) : nombre de nombres premiers inférieurs à n.*

Pour trouver la matrice de décryptage, il suffit d'appliquer la formule ci-dessous :

$$M * D = \frac{1}{DetM} * M^{-1}(\mathrm{mod}\,79) \quad \textbf{(6)}$$

Avec :

- ***MD :*** *matrice de décryptage*
- ***Det M :*** *déterminant de M*
- ***M :*** *inverse de la matrice de chiffrement*

Cette matrice de décryptage sera multipliée avec le vecteur trouvé lors du décryptage RSA, le tout modulo 79 pour trouver une matrice vectorielle que nous appliquerons l'algorithme de permutation voir diagramme 2 afin de retrouver le message envoyé, en utilisant la formule ci-dessous.

$$H = M^{-1} * C_j(\mathrm{mod}\,79) \quad \textbf{(7)}$$

Avec :

- H : Matrice contenant le caractère de départ
- M^{-1} : matrice inverse
- C_j **:** les caractères décryptés

IV. ÉTUDE DE CAS ET TEST DE LA MÉTHODE

Soit le mot **SALBUTAMOL** crypté et décrypté avec une matrice carrée de 10 lignes et 10 colonnes comme suit :

M=

$$\begin{bmatrix} 1 & 3 & 8 & 9 & 1 & 4 & 0 & 0 & 5 & 8 \\ 9 & 8 & 9 & 9 & 2 & 8 & 3 & 2 & 6 & 5 \\ 7 & 1 & 7 & 3 & 5 & 5 & 5 & 1 & 8 & 6 \\ 5 & 4 & 2 & 5 & 5 & 0 & 0 & 0 & 6 & 1 \\ 0 & 5 & 8 & 2 & 2 & 6 & 8 & 2 & 6 & 2 \\ 0 & 9 & 4 & 6 & 2 & 4 & 5 & 6 & 3 & 5 \\ 8 & 1 & 6 & 9 & 9 & 7 & 5 & 0 & 7 & 4 \\ 5 & 5 & 1 & 9 & 0 & 7 & 9 & 4 & 6 & 1 \\ 9 & 9 & 0 & 4 & 6 & 4 & 4 & 6 & 9 & 6 \\ 0 & 9 & 8 & 4 & 1 & 0 & 8 & 6 & 7 & 3 \end{bmatrix}$$

Det = 38416607

IV.1. Chiffrement

Ainsi, H= "***Salbutamol***". Après avoir appliqué l'algorithme de permutation (figure 2) et l'algorithme de correspondance ***(figure 2)*** à H, H devient : **['S', 'B', 'U', 'A', 'L', 'T', 'O', 'L', 'A', 'M'].** Et devient également un vecteur avec les valeurs : **[33 45 56 46 7 64 45 22 31 56].** C'est-à-dire A=12, O=27, L=33 etc... L'application de la formule **(2),** nous conduit à une matrice de lignes.

[62, 33, 32, 5, 45, 34, 49, 53, 61, 36].

En utilisant le chiffrement RSA, ci-dessus, et en choisissant deux grands nombres premiers p et q tels que p=101, q=103 et ***e*** = 7 comme exposant, nous aurons **:** ***n = pq=10403 et (φn) = (p - 1)(q - 1)=10200***, l'inverse ***d*** aura la valeur 8743. En appliquant la formule ci-dessous et l'algorithme de correspondance à notre vecteur ligne, nous trouvons :

[62, 33, 32, 5, 45, 34, 49, 53, 61, 36].

Ceci est équivalent à :

['R', 'S', '9', 'D', 'A', 'v', 'e', 'i', 'Q', '-'].

En appliquant la formule (4), pour le cryptage RSA, nous avons :

[3191, 4742, 2564, 5304, 7746, 7549, 7999, 174, 220, 8770].

3191chiffre pour le caractère R, 4742 pour S, 2564 pour 9 et ainsi de suite**.**

IV.2. Déchiffrement

Après calcul, on trouve que son déterminant est : 38416607. Son GCD (greatest common divisor) avec 79 donne 1. Donc 38416607 a un inverse dans $Z/_{79}$ que nous devrons trouver. En appliquant la formule 5. et en remplaçant e par le déterminant de la matrice modulo 79, on voit que S=1 et i = 27 qui est bien l'inverse de 38416607. En appliquant la formule 6, nous trouvons la matrice de décryptage.

Pour décrypter avec RSA, nous appliquons la formule de (4) et trouvons :

Y =**[3191, 4742, 2564, 5304, 7746, 7549, 7999, 174, 220, 8770].**

[62, 33, 32, 5, 45, 34, 49, 53, 61, 36], qui fournit un caractère :

['R', 'S', '9', 'D', 'A', 'v', 'e', 'i', 'Q', '-'].

C_j est trouvé et multiplié par l'inverse de la matrice de chiffrement selon la formule ci-dessus (7) pour trouver les caractères de départ après application de l'algorithme de permutation 4 :

C_j= [33 45 56 46 7 64 45 22 31 56].

[12.0, 31.0, 30.0, 27.0, 33.0, 7.0, 6.0, 18.0, 22.0, 21.0]

['S', 'B', 'U', 'A', 'L', 'T', 'O', 'L', 'A', 'M'].

['S', 'A', 'L', 'B', 'U', 'T', 'A', 'M', 'O', 'L']

V. ÉTUDE STATISTIQUE

Dans notre étude, nous voulons crypter le mot : SALBUTAMOL en mode ECB et CBC. Et savoir s'il y a une relation entre le cryptage de ce mot en mode ECB et CBC avant et après le cryptage.

Comme le montre le tableau ci-dessous, il n'y a pas de relation linéaire de cryptage de mots SALBUTAMOL entre le mode EBC et le mode CBC avant le cryptage, puisque le coefficient de corrélation entre ces deux modes r=-0, r est proche de 0 et aussi en mode CBC, les caractères à crypter sont XORés avec les caractères initiaux.

Tab. 1. Calcul du coefficient de corrélation r en mode ECB et CBC avant le cryptage

	xi	yi	xi-moy	yi-moy	(xi-moy)(yi-moy)	(xi-moy)2	(yi-moy)2
	62	**3**	21	-45,8	-962	441	2098
	33	**70**	-8	21,2	-170	64	449
	32	**50**	-9	1,2	-10,8	81	1,44
	5	**26**	-36	-22,8	820,8	1296	520
	45	**66**	4	17,2	68,8	16	296
	34	**59**	-7	10,2	-71,4	49	104
	49	**15**	8	-33,8	-270	64	1142
	53	**53**	12	4,2	50,4	144	17,6
	61	**76**	20	27,2	544	400	740
	36	**70**	-5	21,2	-106	25	449
Moyenne	**41**	**49**	**0**	**0**	**-11**	258	582
écart-type	**16,9**	**25**				25,8	58,2
R	**-0**						
EQM	2,95	5,6					

Graphiquement, cette étude statistique peut être présentée comme suit :

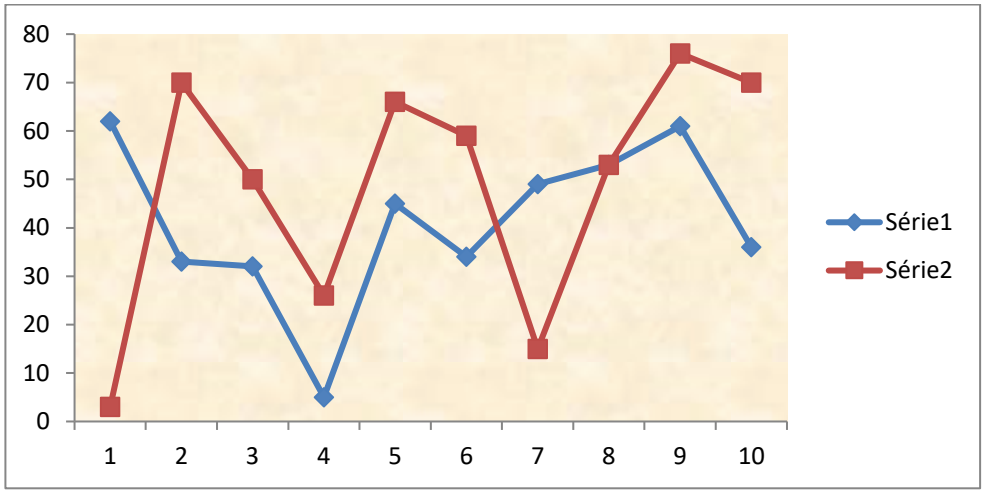

Fig.6 : Graphique de cryptage ECB-CBC avant le cryptage

Tout comme avant le cryptage, il n'y a pas non plus de relation linéaire du cryptage du mot " ***SALBUTAMOL*** " entre le mode EBC et CBC après le cryptage, puisque le coefficient de corrélation entre ces deux modes r=0,1. Comme le montrent le tableau et le graphique ci-dessous.

Tab. 2. Pour le calcul du coefficient de corrélation r en mode ECB et CBC après cryptage.

	xi	yi	xi-moy	yi-moy	(xi-moy)(yi-moy)	(xi-moy)2	(yi-moy)2
	3191	**2187**	-1635	-2423	3960545,25	2672898	5868506,3
	4742	**5867**	-83,9	1258	-105504,25	7039,21	1581306,3
	2564	**2813**	-2262	-1797	4063503,35	5116191,6	3227412,3
	5304	**7578**	478,1	2969	1419239,85	228579,61	8811992,3
	7746	**3602**	2920	-1008	-2942000,8	8526984	1015056,3
	7549	**10007**	2723	5398	14697932,3	7415273,6	29133006
	7999	**503**	3173	-4107	-13030335	10068564	16863342
	174	**174**	-4652	-4436	20633502,5	21640174	19673660
	220	**7497**	-4606	2888	-13299536	21214315	8337656,3
	8770	**5867**	3944	1258	4959705,75	15555925	1581306,3
Moyen	**4826**	**4610**	**0**	**0**	**2035705,25**	9244594,3	9609324,5
écart-ty	**3205**	**3268**				924459,43	960932,45
R	**0,194**						
EQM	**837,8**	**915,7**					

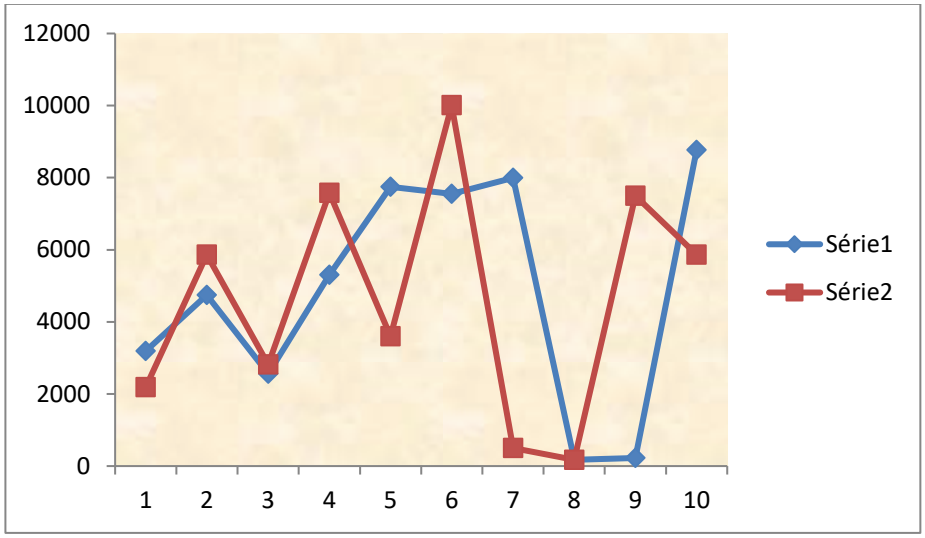

Fig. 7 : Graphique de cryptage ECB-CBC après le cryptage

VI. DISCUSSION

Notre travail consistait à mettre en place un nouveau système de chiffrement hybride basé sur le calcul matriciel et l'algorithme RSA avec l'Alphabet Désordonné. Dans notre système, nous avons utilisé une matrice carrée de taille 10 avec un espace de 79 éléments, c'est-à-dire les 26 lettres de l'alphabet majuscule, minuscules et les caractères spéciaux. Notre système est un système hybride car nous avons fusionné les avantages du cryptage symétrique avec ceux du cryptage asymétrique. Le mode de cryptage utilisé est le CBC (Cipher Bloc Chaining), qui empêche que deux caractères identiques soient cryptés et donnent les mêmes caractères en sortie.

Contrairement à ce que d'autre propose, l'auteur et ses collaborateurs ont également travaillé sur le cryptage de données basé sur des calculs matriciels, mais avec une matrice de taille 2, avec leur système, les données étaient cryptées par blocs de 2 avec un alphabet normal en mode EBC (Electronic code book)[13]. Les résultats qu'ils ont trouvés, ont prouvé que leur système n'était pas efficace, puisque 2 caractères identiques étaient cryptés de la même manière en sortie. Une troisième personne pouvait facilement trouver les informations

[13] S. Kumar H.S., H.T Panduranga. & Naveen Kumar S.K. "Hybrid Approach for Image Encryption Using Hill Cipher Technique". *International Conference on Information Processing*. pp 200–205. DOI: 10.1007/978-3-642-31686-9_23.

cachées en utilisant l'attaque par force brute, car la matrice de cryptage était petite[14].

En revanche, pour notre système, il est difficile de retrouver les informations cachées, car nous avons utilisé une grande matrice, de taille 10. Nos données sont cryptées par blocs de 10 et sont permutées avant le cryptage avec un alphabet désordonné. Nous avons créé un système hybride en ajoutant l'algorithme asymétrique RSA, reconnu internationalement, pour crypter nos données[15].

VII. CONCLUSION ET PERSPECTIVES

Cet article porte sur la mise en œuvre d'un système cryptographique hybride, basé sur le calcul matriciel, après étude, la méthode proposée est efficace dans le sens où un intrus malveillant, utilisant la méthode de force brute, aura des difficultés à récupérer les informations cachées, car notre algorithme utilise une grande matrice avec un alphabet désordonné, en plus de toutes les données sont permutées avant le chiffrement.

Les résultats obtenus après notre étude, montrent la robustesse de notre système qui combine le système cryptographique symétrique et asymétrique. Malgré cela, notre algorithme hybride présente également des failles dans le sens où plus la matrice et la clé choisie sont grandes, plus le temps d'exécution est long. Pour l'avenir, le recours aux courbes elliptiques serait un choix judicieux, car elles fournissent des clés de petite taille, mais garantissent une sécurité élevée.

[14] M. ZEEBAREE, "DES encryption and decryption algorithm implementation based on FPGA," *Indones. J. Electr. Eng. Comput. Sci.* , vol. 18, no. 2, p. 774, mai 2020, doi : 10.11591/ijeecs.v18.i2.pp774-781.

BIBLIOGRAPHIE

1. Courant D., "From kleroterion to cryptology: The act of sortition in the twenty-first century— instruments and practices", *cairn info International Edition*, pp 343-372, 2019.
2. Iniesta C., J. L. Olazagoitia, J. Vinolas, and J.Gros, "New method to analyse and optimise thermoacoustic power generators for the recovery of residual energy," *Alexandria Eng. J.*, vol. 59, no. 5, pp. 3907–3917, Oct. 2020, doi: 10.1016/j.aej.2020.06.046.
3. JACOB. S Thèse de doctorat : " *Protection cryptographique des bases de données : Conception et cryptanalyse. Cryptographie et sécurité* ". Université Pierre et Marie Curie - Paris VI, 2012. Français.
4. Jagadeesh Basavaiah, Audre Arlene Anthony & Chandrashekar Mohan Patil . Visual Cryptography Using Hill Cipher and Advanced Hill Cipher Techniques. Advances in VLSI, Signal Processing, Power Electronics, IoT, Communication and Embedded Systems pp 429–443. DOI: 10.1007/978-981-16-0443-0_34.
5. Karakaya B., "Chaotic System-based Pseudo Random Bit Generator and Post-processor Design for Image Encryption," in *2022 13th National Conference with International Participation (ELECTRONICA)*, May 2022, pp. 1–4. doi: 10.1109/ELECTRONICA55578.2022.9874431.
6. Kuppuswamy P., S. Q. Yahya Al Khalidi Al-Maliki ", A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm", *Bulletin of Electrical engineering and Informatics*. Vol 12, No 2. pp. 1448-1458, DOI: https://doi.org/10.11591/eei.v12i2.4967
7. Madani M., "Medical image encryption based on chaotic maps". *Computers in Biology and Medicine* , vol 43, pp. 1000-1010, 2015.
8. Patel S., Bharath K P, and Rajesh Kumar M, "Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique," *Multimed. Tools Appl.*, vol. 79, no. 43–44, pp. 31739–31757, Nov. 2020, doi: 10.1007/s11042-020-09551-9.
9. Sharath Kumar H.S., Panduranga H.T. & Naveen Kumar S.K. Hybrid Approach for Image Encryption Using Hill Cipher Technique. International Conference on Information Processing. pp 200–205. DOI: 10.1007/978-3-642-31686-9_23.
10. Srinivasan Nagaraj, P. Raju & Kishore Bhamidipati. A New Substitution Block Cipher Using Genetic Algorithm. Conference on Frontiers of Intelligent Computing: Theory and Applications. pp 339–347. DOI: 10.1007/978-3-642-35314-7_39.

11. Srinivasan Nagaraj, P. Raju & Kishore Bhamidipati. Randomized Approach for Block Cipher Encryption. The International Conference on Frontiers of Intelligent Computing: Theory and Applications. pp 551–558. DOI: 10.1007/978-3-642-35314-7_62.
12. VAYEL DOMINUS CARN : La cryptographie Asymétrique avec RSA. Août 2019.
13. Zeebaree S. R. M., "DES encryption and decryption algorithm implementation based on FPGA," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 2, p. 774, May 2020, doi: 10.11591/ijeecs.v18.i2.pp774-781.