LES PUBLICATIONS

# [RECHERCHE]

**Groupe d'Études Scientifiques et Techniques**

## LA NOUVELLE LIGNE MAGINOT : PROTOCOLES CRYPTOGRAPHIQUES ET DÉFENSE NATIONALE A L'ÈRE NUMÉRIQUE


Par Romain D.

LES JEUNES IHEDN

# À PROPOS DE L'ARTICLE

Cet article est le second publié par l'équipe Cyber et Intelligence Artificielle du Groupe d'Étude Scientifique et Technique des Jeunes de l'IHEDN. Créé au début de l'année 2025, ce groupe a pour ambition de rendre accessibles les enjeux techniques, en les reliant aux problématiques doctrinales et géopolitiques.

À l'aube éclatante de l'intelligence artificielle et du traitement massif des données, nos informations — qu'elles soient personnelles, industrielles ou étatiques — se trouvent déjà au crépuscule de leur confidentialité. Tandis que la lumière du progrès se répand, l'ombre grandissante des menaces plane sur notre souveraineté numérique. Celle-ci, qui désormais, est nécessaire à la puissance de l'États, confrontés à des acteurs étatiques et privés toujours plus influents et concurrents.

Dans ce contexte incertain, les méthodes cryptographiques et les protocoles qui leur sont associés apparaissent comme des remparts techniques, souvent méconnus et mal compris du grand public. Pourtant, ils sont essentiels : garants de la confidentialité des données, ils participent à la préservation de notre sécurité, tant collective qu'individuelle. Cet article de vulgarisation tentera, autant que possible, d'éclairer ces concepts fondamentaux, pierres angulaires de notre souveraineté numérique.





**Avertissement**

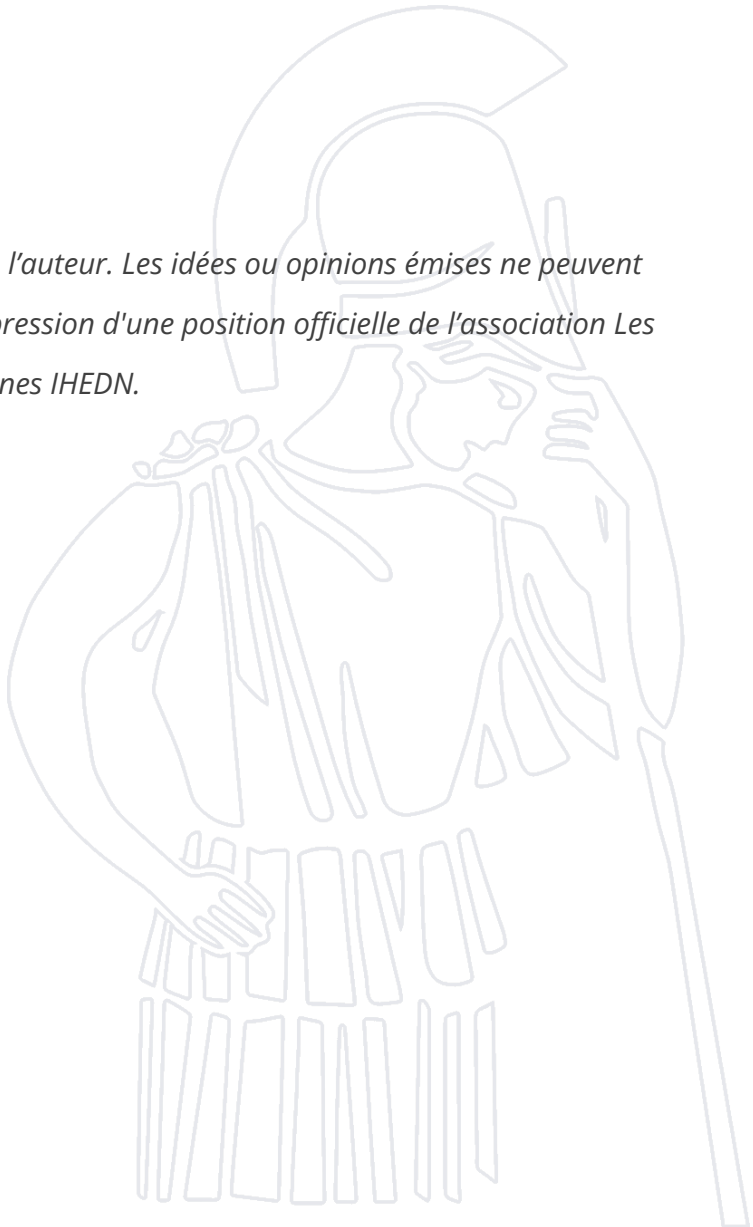
Ceci est un article de **vulgarisation** ; il n'est en aucun cas un article de recherche. **Aucun prérequis n'est nécessaire** pour apprécier l'article. Si vous souhaitez en savoir plus, de nombreux articles discutant de la cryptographie sont présents dans les **sources en note de bas de page.**

# À PROPOS DE L'AUTEUR

**Romain D**. Est étudiant en informatique à l'Université de Rennes, passionné et autodidacte dans le domaine de la cybersécurité. Engagé en tant que Chargé de Mission auprès du groupe Scientifique et Technique en tant que chef de projet Cyber / IA

# Table des matières

*Ce texte n'engage que la responsabilité de l'auteur. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.*



# La cryptographie : protéger l'information depuis l'Antiquité

## Définition

Selon le Larousse, la cryptographie est un *« ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données »*. En décortiquant cette définition, le plus important semble être le mot « chiffrement ». Le chiffrement est l'art de transformer un message (qui n'est pas nécessairement du texte) avec une méthode mathématique afin de le rendre impossible à lire tel quel, ce qui assure alors « l'inviolabilité » de la donnée. La cryptographie permet alors de transmettre des messages de manière sécurisée en s'assurant que seul le destinataire dudit message puisse en prendre connaissance.

La cryptographie a toujours été utilisée au cours de l'histoire[1,2]. Un exemple connu est le chiffrement de César. À l'époque antique déjà, Jules César, lors de la conquête des Gaules chiffrait ses messages, pour transmettre des informations militaires. Aujourd'hui, il existe différents types de chiffrement qui mettent en œuvre différentes méthodes mathématiques permettant, au choix, d'être symétrique, asymétrique ou bien même à sens unique.



## Le chiffrement symétrique

Le chiffrement symétrique est la méthode, sûrement la plus « simple », à concevoir. Il s'agit d'une méthode qui consiste à **partager** une **clef (symétrique) secrète** entre deux ou plusieurs acteurs afin de pouvoir déchiffrer le message. Prenons un exemple concret : imaginons une porte d'un appartement. Si deux personnes ont la clef de cette porte, alors elles pourront discuter dans l'appartement à l'abri des yeux ou des oreilles indiscrètes. Reprenons l'exemple précédent, le **chiffrement de César**, qui consiste à faire un décalage dans l'alphabet en fonction d'un nombre donné. Par exemple, si nous prenons 3 comme clef, alors A deviendra D, B deviendra E, C deviendra F, etc.



[1] HOLDEN, Joshua. *The mathematics of secrets - cryptography from Caesar ciphers to digital encryption*. 2017.
[2] MERCIER, Dany-Jack. *Du chiffrement de César a la mathématique de la carte bancaire*. 2002.

Voici le message que vous devez déchiffrer en code César avec une clé de chiffrement de 7 :
IYHCV

La réponse est à la fin de l'article.

Aujourd'hui, le chiffrement symétrique est bien plus complexe qu'un simple décalage de lettres vers la gauche ou la droite. Ce type de chiffrement se base de nos jours sur le calcul matriciel et d'autres calculs mathématiques (notamment logiques), assez complexes, bien qu'il ne soit pas hors de portée d'un lycéen de comprendre ces concepts[3]. La méthode de chiffrement symétrique la plus en vogue, même s'il en existe bien d'autres, est **l'AES[4,5] (128, 256)**, dont les chiffres après le mot AES peuvent être considérés comme la robustesse du chiffrement, c'est-à-dire la qualité de la serrure dans l'exemple de l'appartement.

## Le chiffrement asymétrique

Le chiffrement asymétrique est un chiffrement où **seul le destinataire du message a la capacité de le déchiffrer**. Imaginons que l'appartement, où se rejoignent nos deux précédentes personnes, soit sur écoute et truffé de caméras. Quelqu'un aurait pu faire une copie de leurs clés. Le secret des conversations ne peut alors plus être assuré. Le chiffrement asymétrique résout cette problématique : il permet à deux interlocuteurs de s'envoyer des messages sans qu'ils soient obligés de partager la même clé.

Afin de mieux comprendre ce concept, reprenons la situation où deux personnes, que nous appellerons désormais Alice et Bob, essaient de communiquer de manière secrète.

Alice va acheter des dizaines de cadenas identiques (ayant la même serrure) et des boîtes métalliques inviolables. Cependant, Alice garde précieusement les clés de ces cadenas chez elle. Alice dispose, pour les personnes qui souhaitent communiquer avec elle, au milieu de la ville, les dizaines de cadenas et de boîtes qu'elle a achetés. Bob écrit sur un papier le message secret qu'il souhaite transmettre à Alice. Puis il met le message, dans

[3] Disponible sur : https://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/indexclesecrete.
[4] FERRADI, Houda. « Introduction à la cryptographie : Chiffrement par bloc (AES) ». *Cours de l'Université Paris* [en ligne], 2016. Disponible sur : https://www.di.ens.fr/~ferradi/coursAES.pdf.
[5] DUTERTE, J.M. « Synthèse AES 128 ». *Cours de cours de l'Ecole des Mines de Saint-Etienne* [en ligne], 2011. Disponible sur : https://www.emse.fr/~dutertre/documents/synth_AES128.pdf.

une des boîtes au milieu de la ville. Ensuite, il prend un des cadenas à disposition et ferme alors la boîte avec. Enfin, Bob envoie la boîte fermée à Alice par la poste. Alice reçoit alors la boite et afin de lire le message ouvre le cadenas avec l'une des clefs qui n'a jamais quitté son domicile.

En termes un peu plus techniques. Les cadenas à disposition de tous sont ce qu'on appelle des **clefs publiques**. C'est-à-dire que tous les **expéditeurs** qui souhaitent adresser un message à un destinataire peuvent se la procurer. Néanmoins, lorsque le message est dans une des boîtes, et fermé par l'un des cadenas, il est impossible pour l'émetteur de le changer. Quiconque n'a pas la clef du cadenas ne peut lire le message, qui est alors chiffré avec la clef publique. Lorsque Alice utilise sa clef pour ouvrir la boîte, celle-ci alors déchiffre le message, avec ce que l'on appelle une **clef privée**, car seul le **destinataire** peut avoir.

Évidemment, derrière cette abstraction de cadenas, de clefs et de boîte, se cachent en réalité des propriétés mathématiques. Celles-ci sont également à la portée de lycéens[6]. La méthode de chiffrement asymétrique la plus utilisée aujourd'hui est la méthode de **chiffrement RSA[7].** Le RSA se base sur la difficulté de **factoriser des nombres premiers** afin de garder un message secret, via une **fonction à sens unique**. Néanmoins, il existe d'autres méthodes de chiffrement asymétrique, comme certaines propriétés **des courbes elliptiques[8,9]**.



## Fonctions de hachages

**Le hachage**, est essentiel dans le monde numérique. Hacher une donnée, est le fait de la faire entrer dans un algorithme afin que celui-ci nous rende un **hash, une unique suite de lettres et de chiffres de taille finie**. Le but de l'algorithme est alors qu'il soit impossible de remonter au message d'origine**,** ce qui est la **non-réversibilité**, tout en évitant le plus possible que deux données aient le même hash, ce qui s'appelle une **collision**.

Un exemple permettra sans doute de mieux illustrer le principe. Supposons qu'Alice souhaite communiquer avec Bob. Pour que Bob puisse s'assurer que le message qu'il

[6] Disponible sur : https://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/indexclepublique.
[7] NITULESCU, Anca. « Cryptosystème RSA ». *Cours de l'Ecole Normale Supérieure de Paris* [en ligne]. Disponible sur : https://www.di.ens.fr/~nitulesc/files/crypto3.pdf
[8] https://culturemath.ens.fr/thematiques/lycee/cryptographie-asymetrique-et-courbes-elliptiques
[9] BAUER, Balthazar ; DONAT-BOUILLUD, Pierre & DURAND, Victor. « Courbes elliptiques et cryptographie ». *Ecole Normales Supérieure de Rennes* [en ligne], 2011. Disponible sur : https://perso.eleves.ens-rennes.fr/~pdonatbo/documents/maths/cryptoEllip.pdf.

reçoit n'a pas été modifié, Alice publie sur un panneau d'affichage public une suite de caractères : il s'agit des premières lettres de chaque ligne du message.

Imaginons maintenant qu'un tiers intercepte le message et y ajoute ne serait-ce qu'un mot. Lorsque Bob reconstruit la suite des premières lettres de chaque ligne, il constate alors une différence avec celle affichée par Alice sur le panneau. Cela lui permet de détecter que le message a été altéré.

Le chiffrement à sens unique est souvent utilisé afin de vérifier l'authenticité d'une donnée, comme vu précédemment, sans pour autant la révéler. Cela permet par exemple de stocker des mots de passe de façon sécurisée en évitant de les stocker « en clair ». Aujourd'hui, la méthode de hachage la plus utilisée est sans doute **SHA256**.

## De la théorie à la pratique : les protocoles, colonne vertébrale de la sécurité numérique

### Qu'est-ce qu'un protocole ?

Un protocole est un terme souvent employé en informatique. Un protocole est un **ensemble de normes qui permettent de communiquer**. Par exemple, cet article est écrit en français, qui a de multiples règles de conjugaison, de grammaire et de syntaxe. Pour toutes les personnes sachant lire le français, cet article peut alors leur communiquer des informations. Un protocole de communication en informatique est assez similaire : il s'agit d'un ensemble de messages qui sont envoyés à un destinataire d'une certaine manière et avec un certain format, pour pouvoir communiquer des informations.

Un **protocole cryptographique** est un protocole particulier qui intègre de la cryptographie. Il s'agit souvent d'un ensemble de règles qui permettent de communiquer entre des personnes (ou des machines**) tout en assurant la confidentialité des données échangées**. C'est-à-dire en chiffrant les informations qui doivent être gardées secrètes (avec les méthodes vues ci-dessus). Cela ne veut pas dire que toutes les étapes du protocole sont chiffrées, seule la donnée qui doit être gardée secrète doit absolument l'être.

Néanmoins, bien que l'on puisse être sûr que les données secrètes sont protégées en l'état, un attaquant pourrait manipuler un protocole afin qu'il puisse déchiffrer les données que l'on souhaite garder secrètes. Afin d'illustrer ces propos, nous allons devoir

voire comment **modéliser** un protocole. La modélisation la plus utilisée est la **notation Alice et Bob**.

Voici un protocole de communication en notation Alice et Bob :

```
Protocole d'exemple :

   1. A -> B : Salut
   2. B -> A : Voici une clef, keyAB
   3. A -> B : {Ce message est secret} keyAB
```

Voici quelques explications :

1. Tout d'abord, le premier message « `A -> B : Salut` » signifie que notre acteur A (pour Alice) envoie (->) à notre acteur B (pour Bob) le message « Salut ».
2. Le second message a deux parties. B envoie à A « Voici une clef ». La seconde partie du message est plus intrigante : `keyAB`. Cette partie est une clé de chiffrement symétrique (voir ci-dessus) qui permettra à A et B de s'envoyer des messages secrets.
3. Enfin, le troisième message est le suivant : {Ce message est secret} $_{keyAB}$. L'indice keyAB indique que le message envoyé est chiffré par la clé symétrique utilisé entre A et B, `keyAB`.

Nous avons vu ici une situation assez simple, mais cela peut être plus complexe avec l'introduction de clés asymétriques ou bien de **nonces**, qui sont des nombres générés aléatoirement que le destinataire doit renvoyer à l'émetteur ; cela permet parfois de s'authentifier, et d'assurer sa fraîcheur du message (voir : Prouver qu'un protocole est sûr).

## Quand le maillon faible n'est pas le chiffrement… mais le protocole

Les vulnérabilités des protocoles cryptographiques souvent lié au protocole en lui-même plus qu'à la méthode cryptographique utilisée. Le protocole permet, parfois, à un attaquant d'accéder au secret échangé : en rejouant certaines parties du protocole, en se faisant passer pour le destinataire, en manipulant plusieurs sessions, ou en abusant de la confusion de type, etc. Ces **failles, dites logiques,** sont alors bien plus complexes à détecter et surtout à corriger.

Désormais, nous allons voir comment un attaquant ou intrus peut accéder et manipuler les messages secrets. Pour cela, nous nous baserons sur le modèle d'attaque le plus repandu, de **Dolev-Yao**[10], qui assume que l'intrus peut intercepter tous les messages et qu'il peut en envoyer, etc. Ce modèle est une abstraction très large et peu réaliste, mais il permet de vérifier l'inviolabilité d'un protocole dans le cas où l'attaquant ait compromis tout le réseau. Nous assumerons également que l'attaquant ne peut faire de la **cryptanalyse,** c'est-à-dire essayer de mettre en défaut les méthodes de chiffrement. Il existe évidemment des modélisations de l'attaquant plus complètes[11].

Sur la base de notre protocole précédent, l'intrus sera modélisé par un acteur « I ». Celui-ci va intercepter et lire les messages entre Alice et Bob, via uniquement la manipulation du protocole de communication. Nous ajouterons ici une nouvelle notation **I(A) (resp. I(B))** qui signifie que l'acteur I **se fait passer pour A (resp. pour B).**

Voici comment l'attaquant va procéder :

```
Protocole vulnérable :

   1. A -> B : Salut
   2. B -> I(A) : Voici une clef, keyAB
   3. I(B) -> A : Voici une clef, keyAI
   4. A -> I(B) : {Ce message est secret}keyAI
   5. I(A) -> B : {Je suis le méchant}keyAB
```

Voici quelques explications sur la manière dont l'intrus a pu avoir accès aux messages échangés entre Alice et Bob et comment celui-ci a pu manipuler la réponse envoyée par Bob.

```
2. B -> I(A) : Voici une clef, keyAB
```

L'attaquant a pu récupérer la clé symétrique keyAB en se faisant passer pour A, et ensuite il a pu envoyer ce message :

```
3.I(B) -> A : Voici une clef, keyAI
```

[10] PROST, Frederic. « Introduction à la sécurité informatique – 5 Modèle Dolev-Yao ». *Cours de l'Université de Grenoble* [en ligne], 2023. Disponible sur : https://lig-membres.imag.fr/prost/M1_MEEF_NSI/Dolev_Yao.pdf.

[11] BERNAT, Vincent. « Théories de l'intrus pour la vérification des protocoles cryptographiques - Réseaux et télécommunications ». *École normale supérieure de Cachan* [en ligne], 2006. Disponible sur : https://theses.hal.science/tel-00132064v1/document.

Dans le but de pouvoir, par la suite, lire le message suivant qu'allait envoyer A, en remplaçant la clé keyAB par sa propre clé keyAI. Alice pense alors envoyer le message secret ci-dessous à Bob avec la bonne clé.

4. A -> I(B) : {Ce message est secret} $_{keyAI}$

Enfin, l'intrus a pu envoyer un message quelconque qui semble secret et, pire, comme venant de A à B avec le message qui suit :

5.I(A) -> B : {Je suis le méchant} $_{keyAB}$

L'exemple pris ici est particulièrement caricatural afin d'être le plus explicatif possible. Cependant, encore aujourd'hui, des protocoles de communication parfois sensibles souffrent de failles de sécurité au niveau de leur protocole, comme on pourra le voir plus bas (Partie : Exemple de manipulation de protocole cryptographique).

## Prouver qu'un protocole est sûr

Pour éviter d'introduire des vulnérabilités dans un protocole cryptographique, une méthode s'impose plus que les autres : la preuve formelle, qui permet de garantir la sûreté du protocole de manière rigoureuse. Néanmoins, même en l'absence de preuve formelle, un protocole doit généralement satisfaire un certain nombre[12] de propriétés de sécurité fondamentales[13] :

- Le **secret** du message que l'on souhaite échanger.

Le secret du message signifie que l'attaquant ne peut pas le lire, sans manipuler le protocole.

- Le message doit être **authentifié**

L'authentification d'un message signifie que l'on peut être sûr, en l'état, que c'est bien l'émetteur qui a envoyé le message.

- Le message doit être **frais**

[12] Certains protocoles ne nécessitent pas la validation de toutes les propriétés. De plus, la liste des propriétés mentionnées n'est pas exhaustive.
[13] GENET, Thomas. « Introduction aux protocoles cryptographiques ». *Cours de l'université de Rennes* [en ligne]. Disponible sur : https://people.irisa.fr/Thomas.Genet/Crypt/cours.pdf.

La fraîcheur d'un message signifie quant à elle que le message a été émis il y a peu de temps. Par exemple, que ce n'est pas un message qui a été expédié lors d'une précédente conversation et que l'attaquant réutiliserai.

- **L'acteur** doit être **authentifié**.

L'acteur authentifié est la combinaison de la fraîcheur du message et de son authentification, afin de pouvoir affirmer que le destinataire reçoit un message de l'expéditeur avec qui il a établi le protocole.

### Preuve formelle de protocole (Optionnel)

Aujourd'hui, dans le milieu de la recherche, la sûreté des protocoles cryptographiques est devenue maitrisée (dans la plupart des cas). Pourtant, les attaques sur ces protocoles peuvent être assez complexes. C'est pour cela qu'afin de détecter les failles de sécurité une méthode existe : la **preuve formelle de protocole**[14,15]. Celle-ci se base sur la **logique du premier ordre**[16,17].

La preuve formelle de protocole commence par la **modélisation** de celui-ci sous une forme logique. Par exemple, si B a une clé symétrique, alors il peut essayer de déchiffrer un message. Néanmoins, cette modélisation doit être particulière, dans l'objectif de simplifier la vérification des protocoles. En effet, les formules logiques doivent être mises sous la forme de **clauses de Horn**, une manière spécifique d'exprimer un prédicat logique.

Après l'étape de modélisation du protocole, vient l'étape de la spécification d'une **propriété de sécurité**. Une propriété de sécurité est également un prédicat logique modélisant soit un **comportement attendu,** comme la réception des messages échangés entre deux acteurs, soit un **comportement non désiré,** comme l'accès au secret par l'intrus.

Enfin, intervient l'étape de **vérification via un prouveur**[18] **logique.** Celui-ci nous permet de démontrer qu'un protocole est sûr ou non en démontrant la **satisfiabilité** des propriétés de sécurité. Une autre possibilité est **l'indécidabilité** des propriétés, car il

[14] LAFOURCADE, Pascal. « Vérifier la sécurité de nos communications ». *Interstices* [en ligne], 2017. Disponible sur : https://interstices.info/verifier-la-securite-de-nos-communications/.
[15] BLANCHET, Bruno. « Verification de protocoles cryptographiques ». *Cours de l'Ecole Normale Supérieure* [en ligne], 2021. Disponible sur : https://bblanche.gitlabpages.inria.fr/talks/ENS21.pdf.
[16]CHATZIDAKIS, Zoé. « Introduction à la Logique ». *Cours de l'Ecole Normale Supérieure* [en ligne], 2015. Disponible sur : https://www.math.ens.psl.eu/~zchatzid/papiers/coursENS.pdf.
[17]PINCHINAT, Sophie. « La logique du premier ordre ». Cours de l'Université de Rennes [en ligne], 2024. Disponible sur : https://people.irisa.fr/Sophie.Pinchinat/LOG/LOGcoursFO.pdf.
[18] En l'occurrence ProVerif. Disponible sur : https://bblanche.gitlabpages.inria.fr/proverif.

existe dans la logique du premier ordre des propriétés indécidables, on ne peut alors que sous certaines hypothèses démontrer la sûreté du protocole.

Voici un exemple de formalisation logique d'une capacité de l'intrus :

Nous modélisons ici le fait qu'un intru connaissant un message et la clef de déchiffrement aura accès au message en clair. Pour cela, il faut un message chiffré par une clef, puis que l'intrus connaisse ladite clef, et il peut alors avoir accès au message. La modélisation logique est alors la suivante :

$$\forall a: agent, \forall m: message\ .\ intru(\{m\}_{Ka}) \wedge intru(Ka) \rightarrow intru(m)$$

*Pour tous les agents (c'est-à-dire les utilisateurs) et pour tous les messages, si l'intrus connaît un message chiffré par la clé de l'agent et s'il connaît la clé de l'agent, alors l'intrus connaît le message.*

La preuve formelle de protocole, relativement simple à mettre en place (même s'il existe certaines limitations), permet alors de vérifier que les protocoles soumis sont exempts de défauts ou non, assurant une absence de failles logiques dans le protocole.

## Exemple de manipulation de protocole cryptographique



Les failles dans les protocoles de communication sont de réelles menaces pour l'intégrité des systèmes d'information, comme l'exploitation d'une faille[19] dans le contrôle à distance de certains ordinateurs via SSH[20]. Cette faille permettait à un attaquant en position d'homme du milieu (MitM[21]), c'est-à-dire d'être intermédiaire entre l'expéditeur et le destinataire (ex. Protocole vulnérable ci-dessus), de manipuler la négociation SSH. Cela en exploitant la gestion des numéros de séquence pour altérer la session sans casser le chiffrement de la communication.

Cependant, ce type de faille logique se retrouve également dans les systèmes de gestion industrielle (OT[22]). En témoigne cette faille[23] de sécurité sur l'un des systèmes de gestion de l'électricité en Europe, qui ne chiffre ni n'authentifie aucune commande de gestion à distance. Cette faille pourrait pourtant, avec un grand « et si », provoquer un

[19] Terrapin (CVE-2023-48795).
[20] *Secure Shell* : Protocole de connexion à distance à un ordinateur.
[21] *Man in The Middle* : Position où l'attaquant obtient des informations en se mettant au milieu du canal de communication. Comme l'exemple précédemment évoqué ou lors de l'interception d'un courrier.
[22] Operational Technologie : Les technologie informatique principalement utilisé par l'industrie.
[23] « Le réseau électrique européen menacé par une faille critique ». Korben [en ligne], janvier 2025. Disponible sur : https://korben.info/faille-securite-reseau-electrique-europe-controle-radio.html.

effondrement sur une partie du réseau électrique européen, provoquer par une variation trop importante due à la mise hors ligne de plusieurs sources du réseau.

Enfin, une autre faille[24] de sécurité bien plus connue est celle des cartes bancaires françaises des années quatre-vingt-dix. En effet, ces cartes à puces étaient vulnérables aussi bien à cause d'une faille cryptographique qu'à cause d'une faille dans leur protocole d'authentification. Cela permettait alors de fabriquer, de manière simple, des « *YesCards* » qui pouvaient payer sans réellement débiter d'argent. Aujourd'hui, ces failles de sécurité ont été corrigées. Même si d'autres sont toujours présentes, celles-ci sont beaucoup plus complexes à exploiter et à mettre en œuvre à grande échelle.

## Cryptographie et guerre : des champs de bataille aux câbles sous-marins

### Secrets de guerre : la cryptographie dans les conflits du XXe siècle

Dans le passé, et aujourd'hui encore, les méthodes et protocoles cryptographiques ont été massivement utilisés dans les confrontations entre États, et la sécurité des communications militaires a toujours été vitale, notamment durant la Seconde Guerre mondiale, où les Alliés ont pu obtenir un avantage stratégique face à l'Axe en décryptant les messages **d'ENIGMA**[25] et du système de chiffrement japonais **PURPLE**[26]. Ces deux systèmes ayant été utilisés respectivement par les Allemands pour les communications militaires notamment entre *U-Boot* (sous-marin) et par les Japonais PURPLE étant une machine ENIGMA modifiée, utilisé pour les transmissions diplomatiques et la transmission d'ordre provenant de l'Etat-Major.

Encore récemment, les États-Unis considéraient les moyens de chiffrement comme des armes de guerre, soumis à de strictes réglementations sur leurs « exportations ». Aujourd'hui, le chiffrement est encore et toujours bien présent, et même de plus en plus abouti. La sécurité d'Internet repose sur des algorithmes de chiffrement comme **SSL/TLS**, permettant la mise en place du **HTTPS** (le petit cadenas vert) et donc de communication sécurisée entre un « client » et un site web.

[24] GENET, Thomas. « Le protocole cryptographique de paiement par carte bancaire ». *Interstices* [en ligne], 2008. Disponible sur : https://interstices.info/le-protocole-cryptographique-de-paiement-par-carte-bancaire/.
[25] WESTERHOFF, Christian & WEIS, Thomas. « 'Britain's best kept secret' : la machine Enigma et le décodage des messages durant la Seconde Guerre mondiale ». 2016.
[26] HATCH, David A. « ENIGMA and PURPLE : How the Allies Broke German and Japanese Code During the War ». 2000.

## Les relations entre États sur écoute

Pour les États, le chiffrement est devenu indispensable, par exemple par l'utilisation de diverses messageries sécurisées, comme *Olvid* ou *Signal*, par les hauts responsables (encore faut-il ne pas ajouter n'importe qui à n'importe quel groupe). Également par la mise en œuvre de diverses méthodes de chiffrement pour la communication diplomatique ou bien pour le stockage de données sensibles. De plus, l'espionnage des câbles sous-marins de fibre optique [27] et l'écoute permanente des signaux électromagnétiques[28] montrent encore une fois l'importance de la mise en place de méthodes et de protocoles cryptographiques robustes, afin de ne dévoiler aucune information qui pourrait aller contre nos intérêts.

## Combat en réseau : sécuriser les systèmes de demain

Enfin, d'un point de vue beaucoup plus concret et proche du combat, l'intérêt du chiffrement et du développement de protocoles de communication sûrs est vital. En effet, la Révolution des Affaires Militaires (RMA) a mené au combat en réseau, déjà mis en application avec le programme SCORPION, dont le but est une mise en réseau limité et une modernisation des systèmes d'armes et de combat de l'Armée de Terre. Le projet TITAN[29], qui est son successeur, a pour objectif de créer un cloud militaire[30]. Or, la mise en réseau de nos systèmes d'armes, de nos unités et de nos centres de commandement[31], tout comme la robotisation du champ de bataille, impose la nécessité de sécuriser les données en transit, mais également les données stockées. De plus, l'hybridation entre les infrastructures civiles et militaires, comme l'utilisation de solutions de réseaux de télécommunication privés[32], accentue cette préoccupation.





---

[27] « Espionnage : les câbles sous-marins qui auraient permis aux États-Unis d'écouter l'Europe ». *FranceInfo* [en ligne], 2021. Disponible sur : https://www.francetvinfo.fr/monde/europe/allemagne/espionnage-les-cables-sous-marins-qui-auraient-permis-aux-etats-unis-decouter-leurope_4645383.html.

[28] « Comment les USA ont réussi à espionner les présidents français ». *Ouest France* [en ligne], 2015. Disponible sur : https://www.ouest-france.fr/monde/nsa-comment-les-usa-ont-espionne-les-presidents-francais-3508058.

[29] « Dossier de presse Eurosatory ». Ministère des Armées [en ligne], 2022. Disponible sur : https://www.defense.gouv.fr/sites/default/files/ministere-armees/Dossier de presse du ministère des Armées Eurosatory 2022.pdf

[30] BOMONT, Clotilde. « Le cloud défense : défi opérationnel, impératif stratégique et enjeu de souveraineté ». *IFRI* [en ligne], 2021. Disponible sur https://www.ifri.org/fr/etudes/le-cloud-defense-defi-operationnel-imperatif-strategique-et-enjeu-de-souverainete.

[31] LYAUTEY, Nicolas. « Le Commandement et le contrôle (*C2*) des opérations multi-milieux multi-champs de haute intensité : vers une nouvelle Révolution dans les affaires militaires (*RMA*) ». *RDN* [en ligne], 2023. Disponible sur : https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=593&cidcahier=1320.

[32] LAGNEAU, Laurent. « Les blindés de l'armée de Terre vont pouvoir utiliser des moyens de communication civils ». *Opex360* [en ligne], avril 2025. Disponible sur : https://www.opex360.com/2025/04/01/les-blindes-de-larmee-de-terre-vont-aussi-pouvoir-utiliser-des-moyens-de-communication-civils/.

C'est pour cela que la mise en œuvre du *Data-Centric Security*[33] (DCS), c'est-à-dire la sécurité des données en elles-mêmes, permettant seulement à la personne ou à un groupe de personnes autorisées de lire des données que l'on appelle labelisés (à la manière de la protection du secret, une donnée ne peut être lu qu'avec l'habilitation et le besoin d'en connaitre), est un enjeu central. Le DCS reste toujours un sujet de recherche, notamment sur le contrôle d'accès mis en difficulté par la décentralisation et l'aspect dynamique des systèmes de combat[34]. Néanmoins, le seul cœur de la sécurité du DCS est bien la cryptographie et les protocoles qui y sont liés.

## Conclusion

### Le futur de la cryptographie

La cryptographie et les protocoles associés ne se résument pas à ce que nous avons abordé dans cet article. Il y a des aspects mathématiques et d'implémentation informatique derrière toutes les méthodes de cryptographie[35].

De même, il y a des aspects de pointe dans ce domaine, comme dans tous les autres, que nous aurions pu aborder, comme la **cryptographie post-quantique**[36,37] . En effet, le champ de recherche du chiffrement post-quantique vise à développer des algorithmes de chiffrement robustes face à l'émergence des ordinateurs quantique. Ceux-ci étant capables de percer certains algorithmes de chiffrement comme RSA (*via* **l'algorithme de Shor**) grâce à des propriétés physiques de la matière, qui permettent de simplifier la factorisation des nombres premiers.

Nous aurions pu également aborder les méthodes de **chiffrement homomorphique**[38,39]. Ces méthodes permettent d'effectuer des opérations directement sur des données chiffrées et de les renvoyer toujours chiffrées avec l'opération effectuée. Cela garantit ainsi la confidentialité des données même par un traitement distant, par exemple dans le cloud.

[33] GRANDISON, Tyrone et *all*. *Elevating the Discussion on Security Management: The Data Centric Paradigm*. 2007.
[34] LEMONNIER, Etienne et *all*. « Analyse des mécanismes de contrôle d'accès pour une approche dynamique et décentralisée du data-centric security (DCS) ». *CESAR*, novembre 2024.
[35] Très bon cours de mathématique appliqué à la cryptographie de l'Université de Lille avec certain aspect informatique. Disponible sur : http://exo7.emath.fr/cours/ch_crypto.pdf.
[36] Disponible sur : https://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/quantique.
[37]BARDET, Magali. « Cryptographie post-quantique : processus de standardisation du NIST et derniers développements, en particulier en cryptographie basée sur les codes ». *AFNIC* [en ligne], 2019. Disponible sur : https://www.afnic.fr/wp-media/uploads/2021/01/Processus-de-standardisation-du-NIST.pdf.
[38] Disponible sur : https://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/homomorphe.
[39] MINAUD, Brice. « Techniques in Cryptography and Cryptanalysis ». Cours du Master Parisien de Recherche en Informatique (ENS et PSL) [en ligne], 2025. Disponible sur : https://www.di.ens.fr/brice.minaud/cours/MPRI/FHE.pdf.

## Une priorité pour la défense nationale

Pour conclure, la cryptographie et les protocoles cryptographiques sont, d'une manière ou d'une autre, l'assurance de notre sécurité — en tant qu'individu, mais également en tant que nation. Aujourd'hui, le développement de méthodes cryptographiques, ainsi que le développement de nouveaux protocoles sûrs, est ce qui nous permettra demain de défendre notre nation face à des attaques non-cinétique, fer de lance de la guerre basée sur les effets. La recherche dans ces domaines est plus que nécessaire : elle est vitale dans un monde où les échanges de données sont de plus en plus grands, encore plus dans un contexte international d'espionnage à outrance et de gestion des conflits entre États par la force.

La réponse est : BRAVO !







publication@jeunes-ihedn.org