

**Association
des
Réservistes du Chiffre
et de la
Sécurité de l'Information**



- **L'ARCSI est une des principales associations françaises dans les domaines de la cryptologie et de la sécurité numérique.**
- **C'est la plus ancienne et la seule** à faire le pont entre l'histoire de la science du secret (les grandes figures du Chiffre, les procédés, les évènements liés à un fait cryptologique) et les techniques modernes (électronique, informatique, algorithmique) de protection ou d'attaque de l'information.
- **Créée en 1928** par les officiers de réserve du Chiffre, celle-ci, suite aux évolutions techniques et à la généralisation du besoin de protection s'est ouverte progressivement à tous les milieux. Elle est forte d'environ **350 membres**.
- **Elle regroupe une somme considérable de talents et de compétences :** mathématiciens et cryptologues, ingénieurs, enseignants, chercheurs et techniciens spécialistes de cryptologie, de sécurité informatique et/ou de cybersécurité mais aussi juristes, historiens ou journalistes. Elle compte en outre **plusieurs membres étrangers parmi lesquels des sommités mondiales.**



Ses activités :

Des échanges d'information nombreux et de qualité.

- Ceux-ci sont permanents entre les membres tous animés du besoin de partager leurs connaissances et leur expérience. Ces échanges se font soit à l'occasion de rencontres amicales soit via des listes de diffusion.
- La direction de l'ARCSI assure quant à elle :
 - La mise à jour permanente de la rubrique actualités du site WEB
 - La diffusion de deux lettres de veille, l'une hebdomadaire sur le site de l'ARCSI, l'autre sur une liste de diffusion. Sans préjudice des informations fournies par des veilleurs occasionnels et attentifs...

L'organisation de manifestations:

- **Annuelles** : ce sont les « Rencontres de l'ARCSI » sous forme de colloque de grande réputation généralement dans un lieu prestigieux tel que la BnF.
- **Mensuelles** sous forme de conférences intitulées « Les lundi de la cybersécurité » en partenariat avec l'université de Paris
- En outre l'assemblée générale de l'ARCSI est souvent l'occasion d'entendre une ou deux conférences.
- Tous ces évènements relayés sur certains réseaux sociaux dont LinkedIn, font l'objet de captures vidéo mises en ligne sur notre chaîne **Dailymotion**



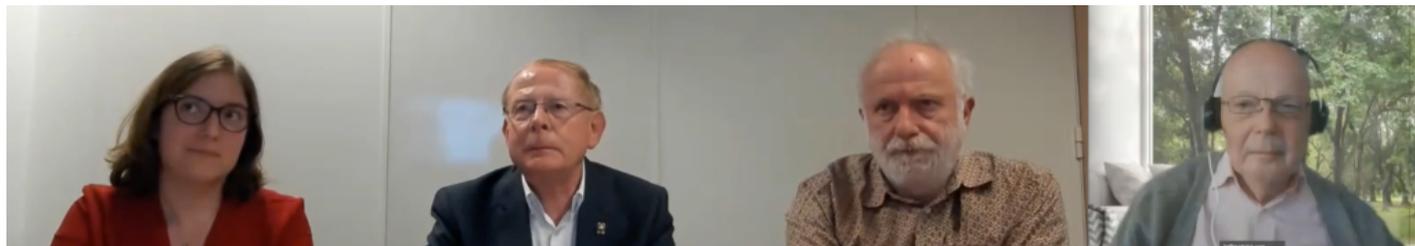
La participation aux grands évènements du domaine, avec tenue d'un stand d'information et une animation

- Le FIC de Lille « forum international de la cybersécurité »
- L' « European Cyber Week » de Rennes
- Le Hack à Paris
- Les GS Days en partenariat avec GlobalSecurityMag à Paris
- Le Salon de la « Culture et des jeux mathématiques » Place St Sulpice à Paris :



Une manifestation exceptionnelle en 2022: L'ARCSI au 18^{ème} symposium de l'histoire de la cryptologie organisé par la NSA

- Le 20 mai 2022, pour la première fois l'ARCSI est intervenue dans ce cénacle prestigieux pour y présenter les hauts faits de la cryptologie française au cours des trois derniers siècles.
- Le panel comprenait: Agathe Couderc, Jean-Louis Desvignes, Philippe Guillot et Jean-Jacques Quisquater. La vidéo est accessible sur Dailymotion.



Exemples de thèmes des « lundi de la cybersécurité »

- "Parler de Cybersécurité au décideur ? »
par Lubna Brioual
- "La cybersécurité peut-elle être efficace ? »
par Solange Ghernaouti
- "Sécurité et cryptographie existent-elles ? »
par Jean-Jacques Quisquater
- "le "SASE", ou Secure Access Service Edge" par Keren Bismuth
- "Les attaques par canaux cachés » Par Jean-Jacques Quisquater



Les dernières « Rencontres de l'ARCSI » :

- 2022 : L'épopée de la carte à puce et son avenir+ hommage à Michel Ugon
- 2019 : La confiance dans notre monde numérique peut-elle renaître ?
- 2018 : L'année des 90 ans de l'ARCSI: La cryptologie, de la Grande Guerre au post-quantique.
- 2017 : Messageries et Systèmes de confiance
- 2016 : La dépendance numérique



Des activités patrimoniales :

Mettant à profit sa riche collection de matériels et de documents anciens l'ARCSI a participé à plusieurs grandes expositions :

- 2022 : Exposition d'une Enigma au Musée canadien de Juno Beach et au musée Champollion de Figeac
- 2019 : Shannon au Musée des Arts et métiers
- 2016 : TOP Secret au Mundaneum à Mons en Belgique
- 2016 : La carte à puce au Musée des Arts et Métiers
- 2015 : Le secret de l'Etat aux Archives nationales à Paris
- 2012 : Cryptologie, La science du secret au Musée des Transmissions à Rennes

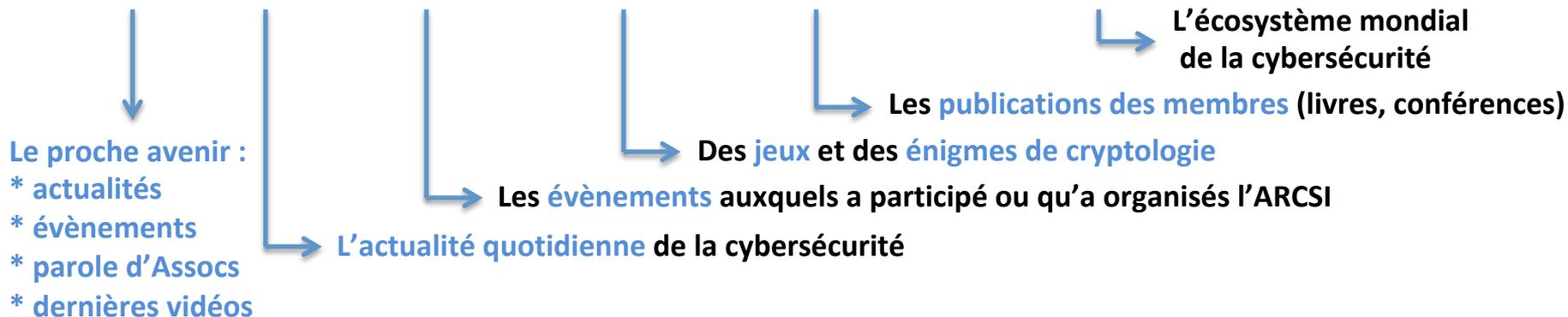


Des publications réalisées par l'ARCSI

- **Un bulletin annuel** réservé aux membres, un lien important entre toutes les générations. Ouvrage de référence pour de nombreux chercheurs
- **Des bulletins hors série** consacrés à un thème particulier.
Ex: les Décryptements d'Enigma par le Gal Ribadeau Dumas.
- **De nombreux ouvrages de nos membres.** Exemples:
 - « La cybersécurité par les nombres », de Pierre-Luc Refalo
 - « Au-delà du Bitcoin » de Jean-Paul Delahaye
 - « La Bible des codes secrets » d'Hervé Lehning



Son site internet : <https://www.arcsi.fr>



ACTUALITÉS

Pour savoir ce qu'il se passe d'important en cryptologie et sécurité de l'information



11 Novembre
2022

Le 22 novembre se tient la 13^{ème} édition des "GS Days", Journées Francophones de la Sécurité

« Convaincre sans contraindre », tel est le slogan de GS Days, Journées francophones de la sécurité, des administrateurs, experts sécurité, les RSSI, DSI et proposer, dans un même espace, plusieurs cycles de conférences, en collaboration avec l'ARCSI, sous encore temps de s'inscrire !

Pour en savoir plus, voir l'article de [gsdays.fr](#).

JEUX & ÉNIGMES

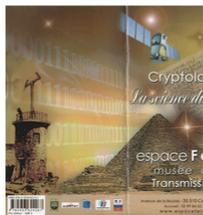
Sur cette page, vous pourrez trouver des jeux et des énigmes de cryptologie, afin de vous familiariser avec la richesse de la cryptologie. Soit également présentés quelques jeux de réflexion. Enfin, vers la chaîne DailyMotion de l'ARCSI vous permettrez de visionner diverses présentations faites par les membres de l'Association.

Indispensables : Les grandes figures de la Cryptologie, et l'histoire de vous un(e) spécialiste du domaine.

Les grandes figures de la Cryptologie



L'histoire de la Cryptologie



de Hill
Japonais JN-25
allemand ADFGVX
avec ENIGMA
allemand de UBCHI
de Bazeries
le de stéganographie

LE CHIFFRE DU MOIS : BELLAZO

Le "Passage de Gué"

Place à quelques énigmes péle-méle

Quelques péripéties de l'Histoire...

ARCSI ont également réalisé des conférences passionnantes sur les technologies et des aspects liés à la cryptologie, disponibles sur notre chaîne vidéo [DailyMotion](#) ! Vous conseillons :

- Le fonctionnement de la grille tournaute de Fleissner
- Le fonctionnement de l'algorithme RSA
- Le rôle de l'unité de chiffrement...

ÉCOSYSTÈME DE LA CYBERSÉCURITÉ

Francis BRUCKMANN
Dernière mise à jour 12/6/2022

D'une manière générale, la cybersécurité englobe tous les moyens qui permettent d'assurer la protection et l'intégrité des données, matérielles ou immatérielles, de l'infrastructure numérique. Elle concerne la souveraineté numérique, les enjeux économiques, stratégiques et de sécurité des systèmes.

ANSSI
DRM
CERTIF
CSN
ENISA
FBI
GCHQ
ICOM
ISCOM
M3AAWG
NCSD
UN/CGE
WOCMA
ARCSI
CLUSIF
CERT-EU
CICS
COMCYBER
BSI
ENISA
CERTIF
GCHQ
ICOM
ISCOM
M3AAWG
NCSD
UN/CGE
WOCMA
ARCSI
CLUSIF
CERT-EU
CICS
COMCYBER
BSI

Ouvrages de Cryptologie les membres de l'ARCSI vous conseillent

Vous trouverez ici une liste non exhaustive d'ouvrages de référence en cryptologie, conseillés par des membres de l'ARCSI spécialistes de ce sujet.

N'hésitez pas à consulter également la rubrique "publications" de ce site et les ouvrages publiés par nos membres.

À la Une



La Bible des codes secrets

Hervé LEHNING
Editions Flammarion - sortie le 6/11/2019



History of Cryptography and Cryptanalysis

Codes, Ciphers, and Their Algorithms

John F. DOOLEY
Ed. Springer - en anglais - 1^{ère} édition août 2018



Codes, Ciphers and Spies

Tales of Military Intelligence in World War 1

PUBLICATIONS de MEMBRES

À la Une : les dernières publications



Conférence des "Lundi de la Cyber": "Parler de cybersécurité au décideur"
Lubna BRIDUAL - 10/2022



La Cybersécurité par les nombres
Pierre-Luc REFALO
Les métiers du futur - 10/2022



Conférence des "Lundi de la Cyber": "La cybersécurité peut-elle être..."
Lubna BRIDUAL - 09/2022

Bitcoin

La Blockchain et des cryptomonnaies
LAHAYE
Jacques Quilquater
D - 8/2022

Le vocabulaire de la cryptologie

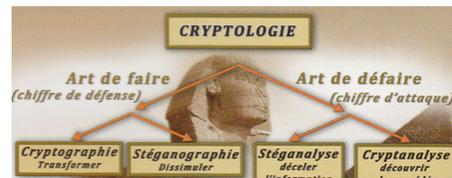
termes et définitions

Depuis l'antiquité, les hommes ont éprouvé le besoin de protéger certaines informations qu'ils voulaient garder secrètes notamment lorsque celles-ci devaient voyager. Différentes techniques furent utilisées parmi lesquelles la **cryptographie**, ou **art (ou science) des écritures cachées ou secrètes**, occupa bientôt une place de choix dès que l'écriture se démocratisa.

La crainte de voir les messages interceptés fut à l'origine du développement de procédés le plus souvent appelés **codes** ou **chiffres**.

Le terme de **cryptologie**, étymologiquement la « science du secret », très récent, rassemble désormais l'ensemble des techniques cryptographiques de protection et d'analyse de leurs failles. La cryptologie concerne la protection de toutes les formes d'information (écrits, images, sons, données de toute nature), et s'intéresse autant au "défenseur" qu'à l'attaquant.

On peut ainsi schématiser les domaines qu'elle regroupe :



Venez y trouver :

- Les **meilleurs ouvrages à découvrir**
- Des **dossiers** sur l'histoire de la Cryptologie
- Des dossiers captivants sur le monde de la Cryptologie
- Le vocabulaire des « initiés »
- Des **Jeux et des Enigmes**
- Et sur notre chaîne Dailymotion **de nombreuses vidéos** :



Les partenaires de l'ARCSI

THALES

LA
BANQUE
POSTALE

THEGREENBOW

IDEMIA

HS2
Hervé Schauer Sécurité

IDECSI

Quarkslab
SECURING EVERY BIT OF YOUR DATA

G·ECHO
sécurité des systèmes d'information

Citalid

CAP'TRONIC
Systèmes électroniques
et logiciel embarqué

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

le cnam

CNIL
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

orange™



{BnF

Forum
ATENA



Pour nous rejoindre et participer à nos activités, c'est simple :



C'est ici !

