Le digital dans les Alpes du Sud :
Sécuriser son informatique en 2025

Patrice Roux

Laurent Céard

Jean-Jacques Brucker

Alpes Conseil Informatique
DEPUIS 1978

Sun Valley Systems

foopgp.org

digit'alpes DU SUD
COLLECTIF DU NUMÉRIQUE ALPES & PROVENCE

CCI PROVENCE ALPES CÔTE D'AZUR

CCI ALPES DE-HAUTE-PROVENCE

CCI HAUTES-ALPES

DOCAPOSTE

LA POSTE GROUPE

Trois piliers importants de la Cybersécurité

Technique

Exemple : Firewall, droits d'accès, chiffrement.

Juridique

Exemple : RGPD (Règlement général de la protection des données)

Organisationnel

Exemple : RSSI (Responsable de la sécurité des systèmes d'information)

Sécuriser son informatique en 2025 : Panorama

Système d’information :

Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information

Attaques numériques :

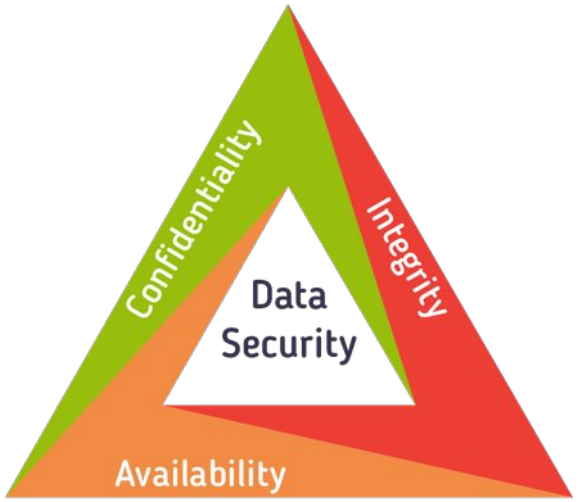
Une cyberattaque désigne un effort intentionnel visant à voler, exposer, modifier, désactiver ou détruire des données, des applications ou d'autres actifs par le biais d'un accès non autorisé à un réseau, un système informatique ou un appareil numérique.

Nouvelles menaces :

* Explosion des solutions « IA »
* Crises géopolitiques => cyberespionnage accru
* Surveillance
* Techno-féodalisme

3

La Triade CIA (CID en FR)



[Confidentialité]

[Intégrité]

[Disponibilité]

Sécuriser son informatique en 2025 : sécuriser ses données

Confidentialité

Utilisation du moindre privilège

Authentification forte

Chiffrement des données

Mise en place d'outils de surveillance

Intégrité

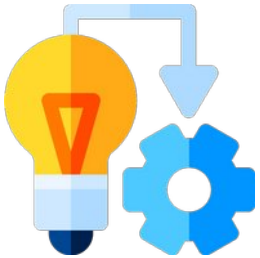
Empêcher les modifications abusives

Mise en place d’une signature électronique

Disponibilité

Mise en place d’un plan de reprise d’activité

Mise en place de redondance (serveurs, Internet)



Moyens à mettre en œuvre

Évaluer les risques

Sauvegarder les données importantes

Sécuriser les accès, chiffrer les données sensibles

Utilisation de mots de passe

DASHLANE

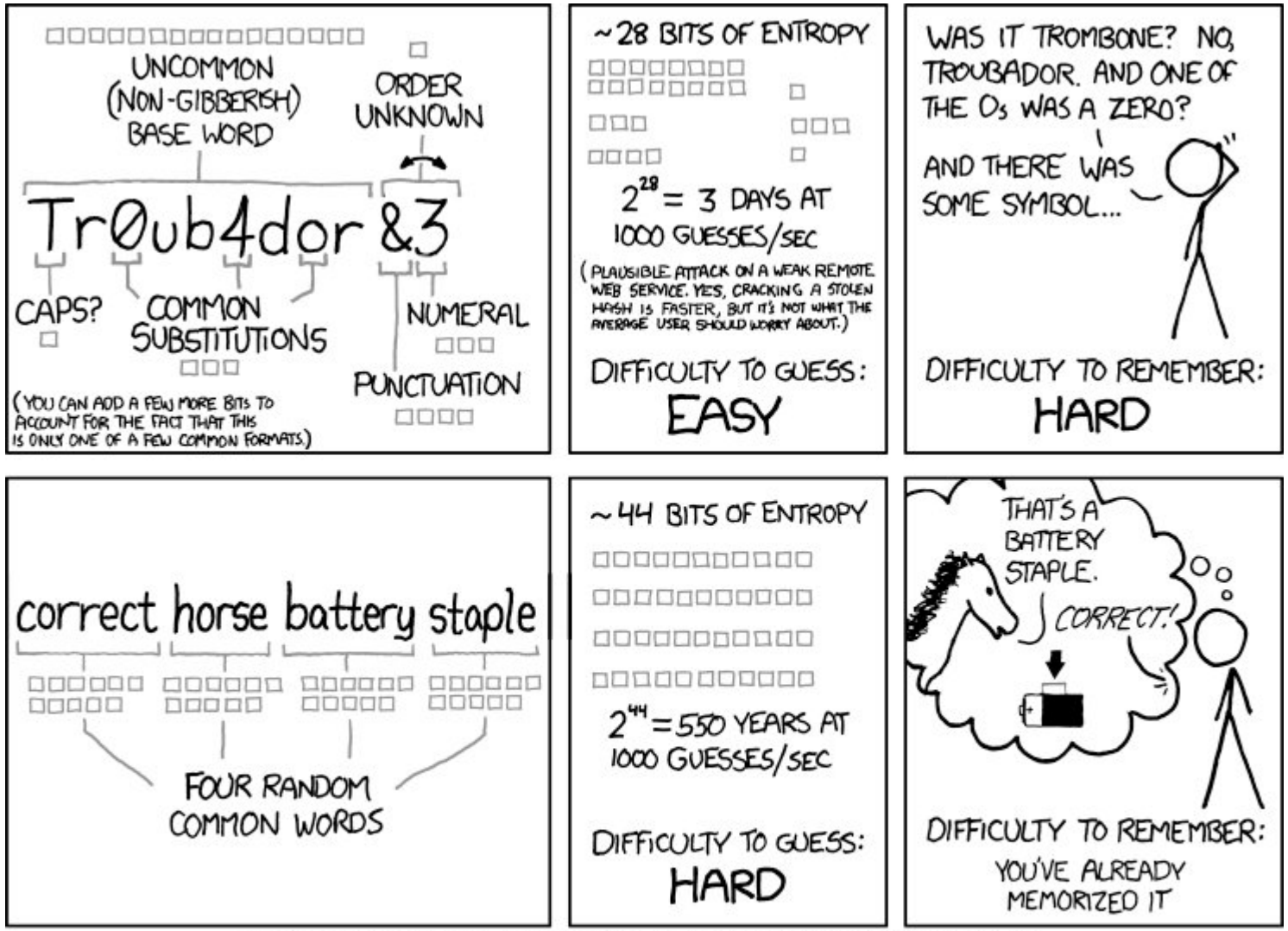
KEEPER
Cybersecurity Starts Here®

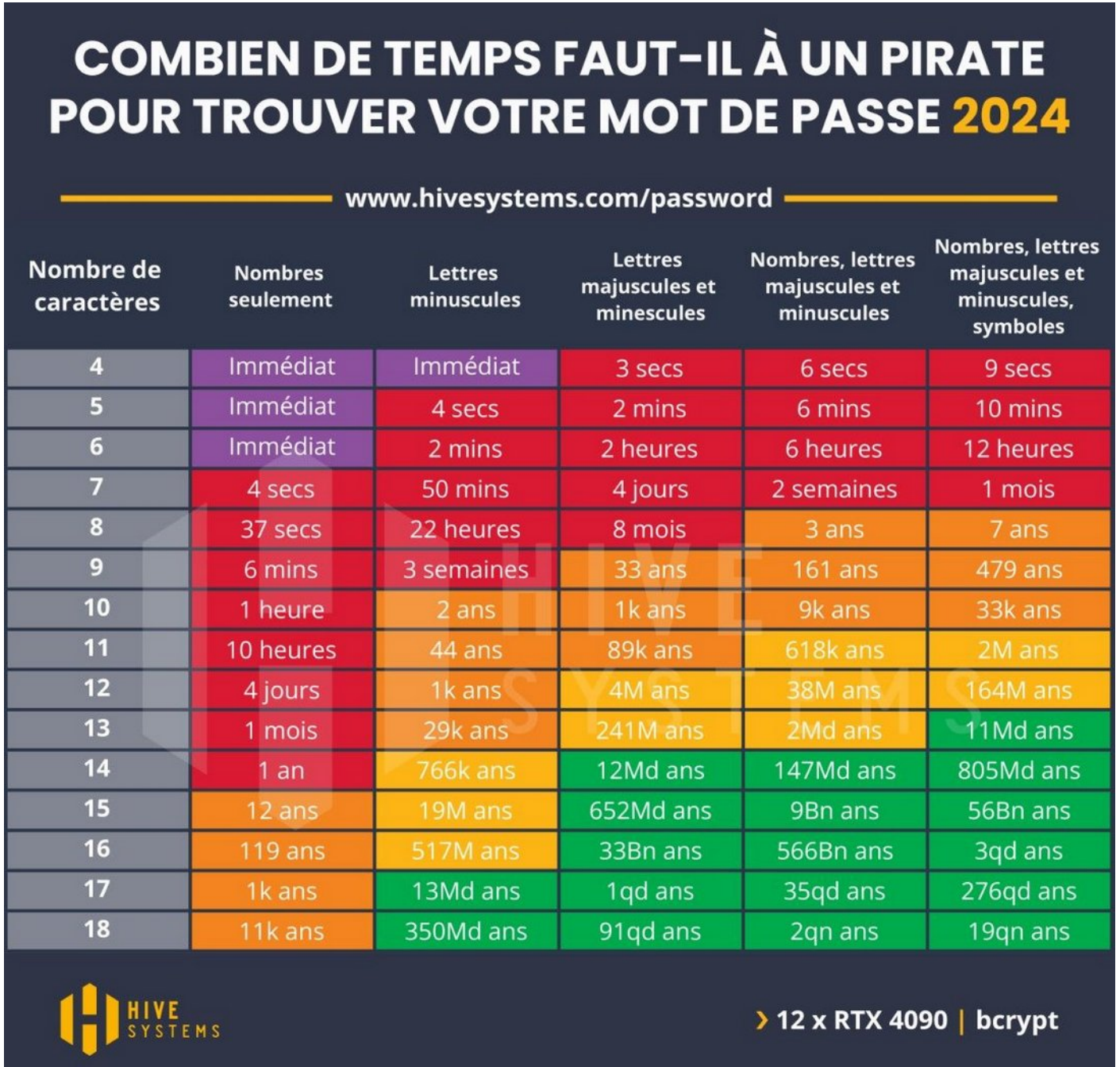
KeePass

bitwarden

Utilisation d'une clé de sécurité

Sécuriser son informatique en 2025 : utiliser de « bons » mots de passe





COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE 2024

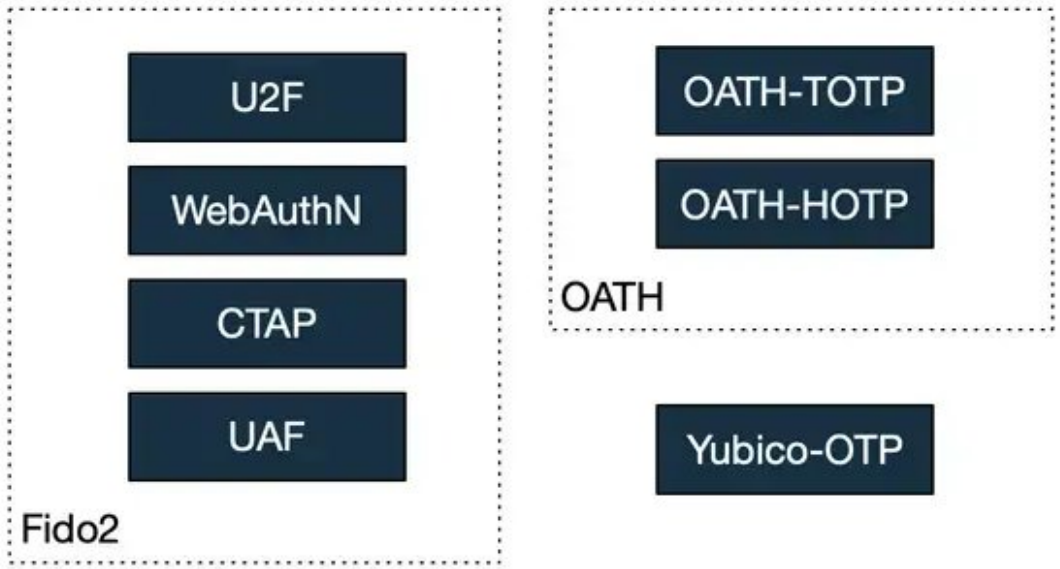
www.hivesystems.com/password

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minesculles	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans
17	1k ans	13Md ans	1qd ans	35qd ans	276qd ans
18	11k ans	350Md ans	91qd ans	2qn ans	19qn ans

HIVE SYSTEMS

› 12 x RTX 4090 | bcrypt

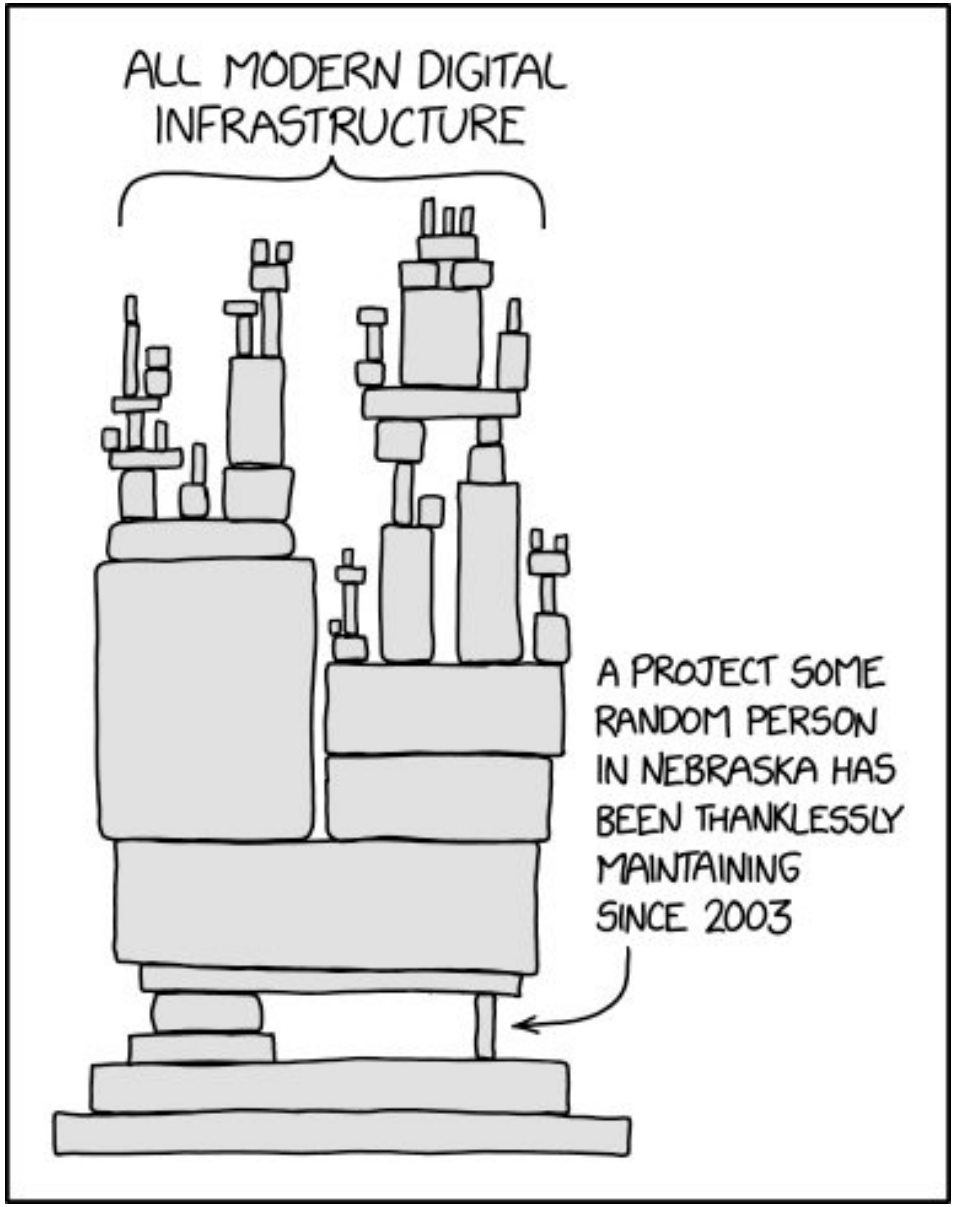
Sécuriser son informatique en 2025 : Les principaux protocoles



OpenPGP

Open Authentication (OATH) : RFC 4226 RFC 6238 RFC 6287

RFC 3156, RFC 9580, RFC 5581, RFC 6091, RFC 6637, et plus encore


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Sécuriser son informatique en 2025 : Différentes clés de sécurité

YubiKey 5 Series

Nitrokey 3 Series

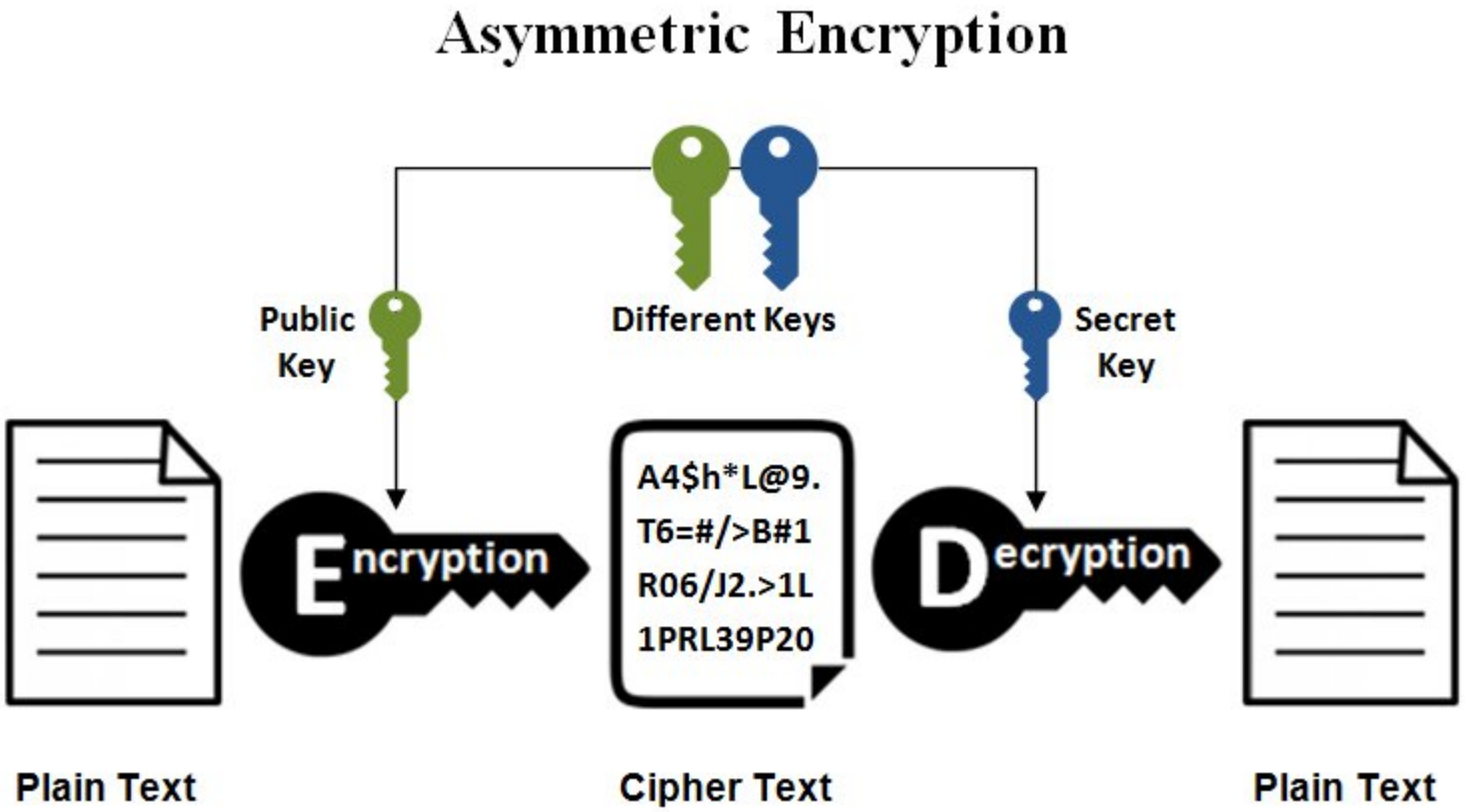
OnlyKey CryptoTrust

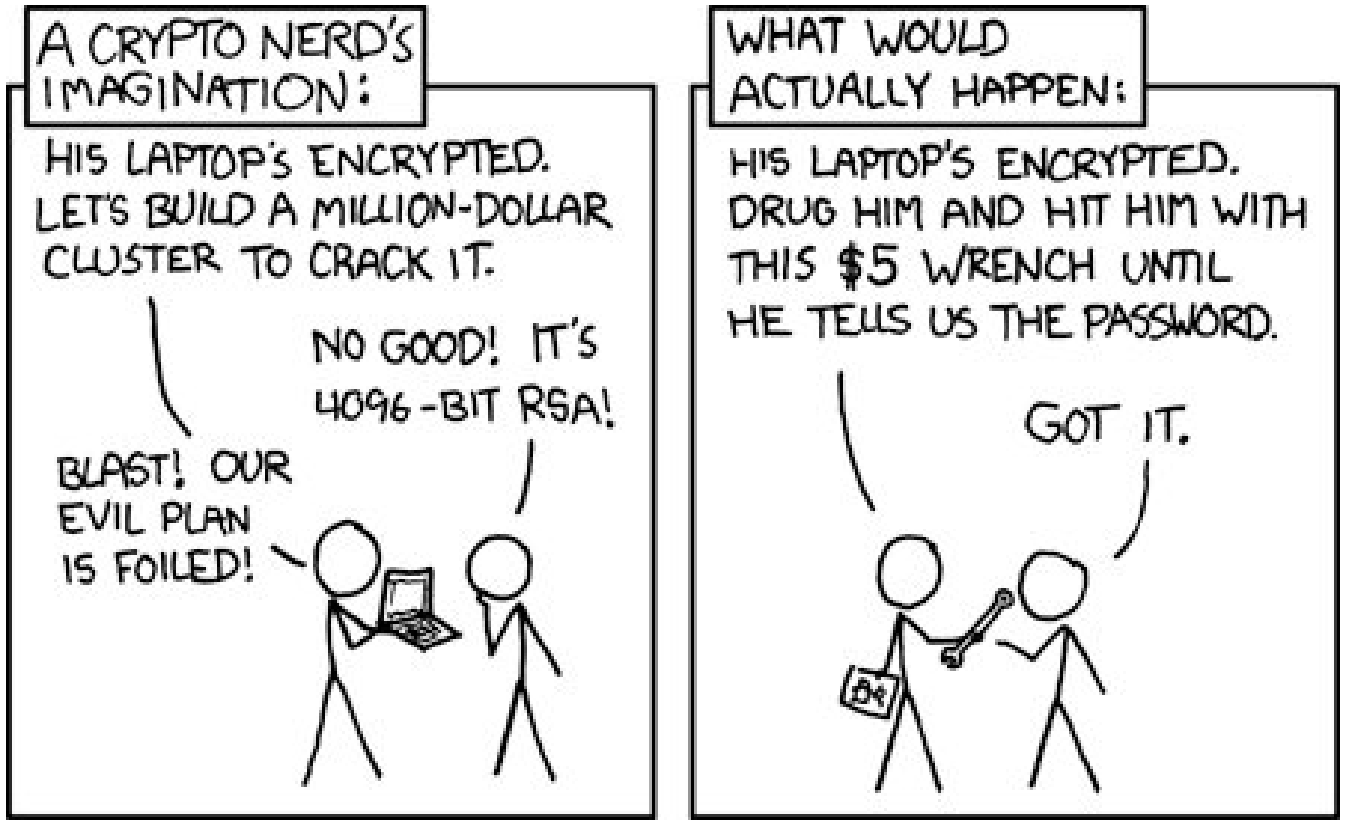
Neowave Winkeo

Sécuriser son informatique en 2025 : Comparatif Protocoles

	Static passwords	Yubico OTP	OATH TOTP	FIDO U2F	FIDO2 (WebAuthn)	S/MIME (X509)	OpenPGP
Authentication	YES	YES	YES	YES	YES *main use: web*	NO	YES *main use: ssh*
Signature	NO	NO	NO	NO	NO	YES	YES
Decryption	Symmetric	NO	NO	NO	NO	Asymmetric	Asymmetric
PKI						Hierarchy of Certification Authorities	Web of Trust

(Rappel sur la cryptographie asymétrique)





* Interface Chaise-Clavier
* Risque zéro
* 0-Days, CVE.
* Anonymat
* Impunité

Qu’est ce que l’ ANSSI

- **ANSSI** (Agence nationale de la sécurité des systèmes d'information)
- Autorité nationale en cybersécurité en France.
- Coordonne les politiques de cybersécurité à l’échelle nationale.
- Joue un rôle clé dans la défense des infrastructures publiques et privées.
- Travaille en collaboration avec des partenaires européens et internationaux..

Surveillance du trafic entrant / sortant

Le firewall, outil essentiel dans la surveillance de votre trafic, actuellement le seul certifié par l'ANSSI est Stormshield.

STORMSHIELD

L'IA : Ami ou Ennemi en cybersécurité ?

- **L'IA accentue les risques** :
  - Automatisation des attaques.
  - Prolongement et sophistication des menaces.
- **L'IA comme alliée** :
  - Détection automatisée des menaces.
  - Aide à l’analyse des logs pour identifier les failles de sécurité.

Gestion des logs et Détection

- **Trop d'alertes, trop peu de temps** :
  - Les équipes de sécurité sont submergées par un volume croissant d'**alertes** et d'événements de sécurité.
  - Difficulté à prioriser les menaces sérieuses parmi des milliers de logs générés quotidiennement.
- **Manque de visibilité** :
  - Beaucoup d'entreprises peinent à avoir une **vue d'ensemble** claire sur leurs systèmes, ce qui complique l'identification rapide des incidents de sécurité.
  - Des failles peuvent passer inaperçues pendant des semaines voire des mois, amplifiant leur impact.
- **Évolutivité** :
  - L'augmentation des sources de logs (applications, systèmes, réseaux) complexifie la gestion.
  - Les infrastructures traditionnelles ne sont souvent pas capables de traiter le volume et la variété des logs générés aujourd'hui.

Logiciels d ’analyses

Splunk, IBM Qradar, Elastic Stack (ELK Stack) avec X-Pack, SolarWinds Log & Event Manager (LEM), Azure Sentinel

- **Détection des anomalies** : L'IA peut identifier des comportements ou des événements inhabituels dans les données de logs.
- **Réduction des faux positifs** : Les algorithmes de machine learning peuvent aider à réduire le nombre de fausses alertes en apprenant des événements passés.
- **Prédiction des incidents** : L'IA peut anticiper des incidents futurs en fonction des tendances historiques et des schémas comportementaux.
- **Automatisation des réponses** : L’IA permet d’automatiser les actions correctives, réduisant ainsi les délais de réponse aux incidents.
- **Corrélation des événements** : L'IA aide à corréler des événements provenant de sources différentes pour fournir une vue plus complète des menaces

S'informer et se former en continu : La clé pour rester en sécurité

Consulter régulièrement le site de l'**ANSSI**

Abonnement aux bulletins de sécurité : Suivez des **bulletins de sécurité** émis par des autorités comme l'ANSSI, le CERT-FR ou les blogs spécialisés pour ne pas manquer les nouveautés.

SecNumAcademie : Une plateforme en ligne gratuite où vous pouvez suivre des modules de formation dédiés à la cybersécurité. Accessible à tous, du novice à l'expert.

La presse spécialisée : une source inépuisable de savoir, newsletter etc..

S’auto-former avec des plateformes de e-learning

« Apprendre à son rythme »

MOOCs : Inscrivez-vous sur des plateformes comme **Coursera**, **Udemy**, ou **OpenClassrooms** qui proposent des cours en cybersécurité, allant de l’initiation à des niveaux plus avancés.**Coursera** : Cours sur la cybersécurité pour débutants avec certification officielle.

•**Udemy** : Des centaines de formations à la demande sur des sujets tels que la gestion des risques, le hacking éthique, et la cryptographie.