La Cryptographie

Par Victor, Gabriel et David

Histoire de la cryptographie

-Chiffre de César

-ROD 13

- Vigenère

CODAGE

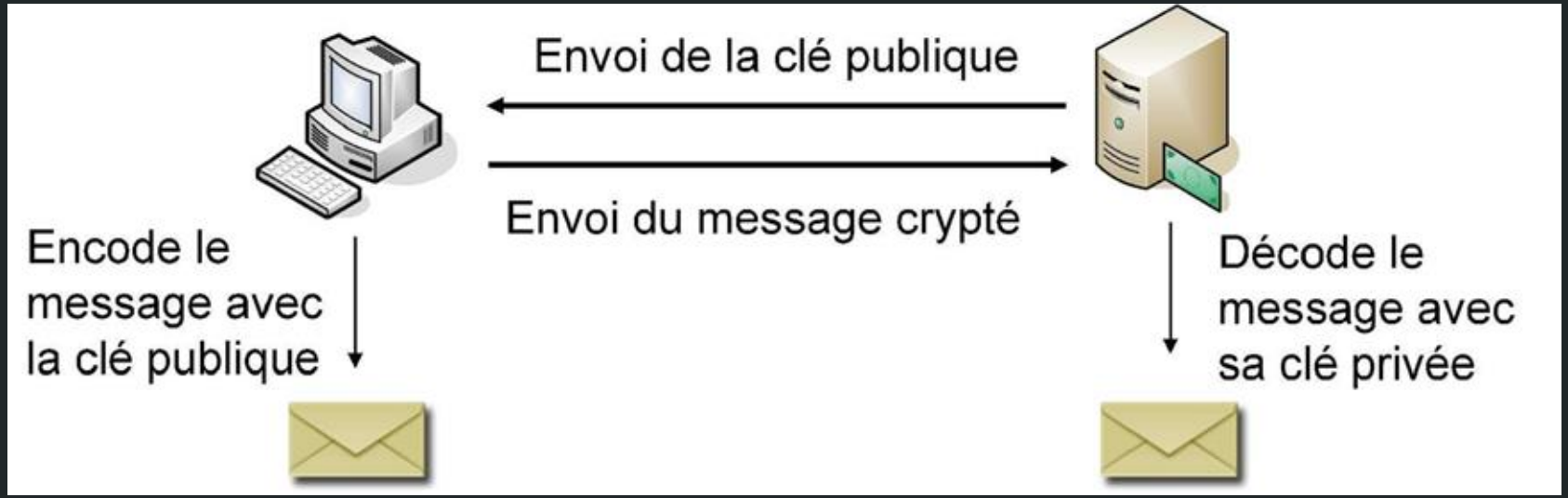
Message	B	O	N	J	O	U	R
	2	15	14	10	15	21	18
Chiffres + 3	5	18	17	13	18	24	21
Message codé	E	R	Q	M	R	X	U

DECODAGE

Message codé	E	R	Q	M	R	X	U
	5	18	17	13	18	24	21
Chiffres -3	2	15	14	10	15	21	18
Message décodé	B	O	N	J	O	U	R

Rappel : chiffrement symétrique ou à clé secrète

E (Fonction de chiffrement) et D (Fonction de déchiffrement): Fonctions inversibles et efficaces
K: Clé secrète ou symétrique
C: Le message chiffré

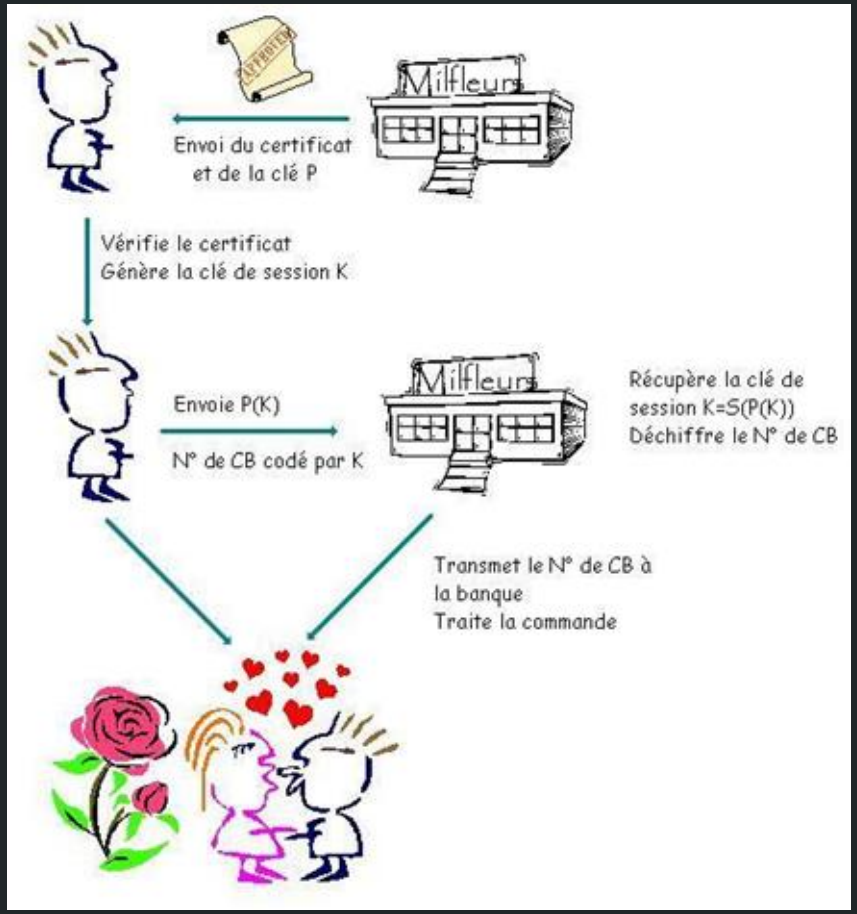

Envoi de la clé publique
Envoi du message crypté
Encode le message avec la clé publique
Décode le message avec sa clé privée

L’utilisation actuelle de la cryptographie

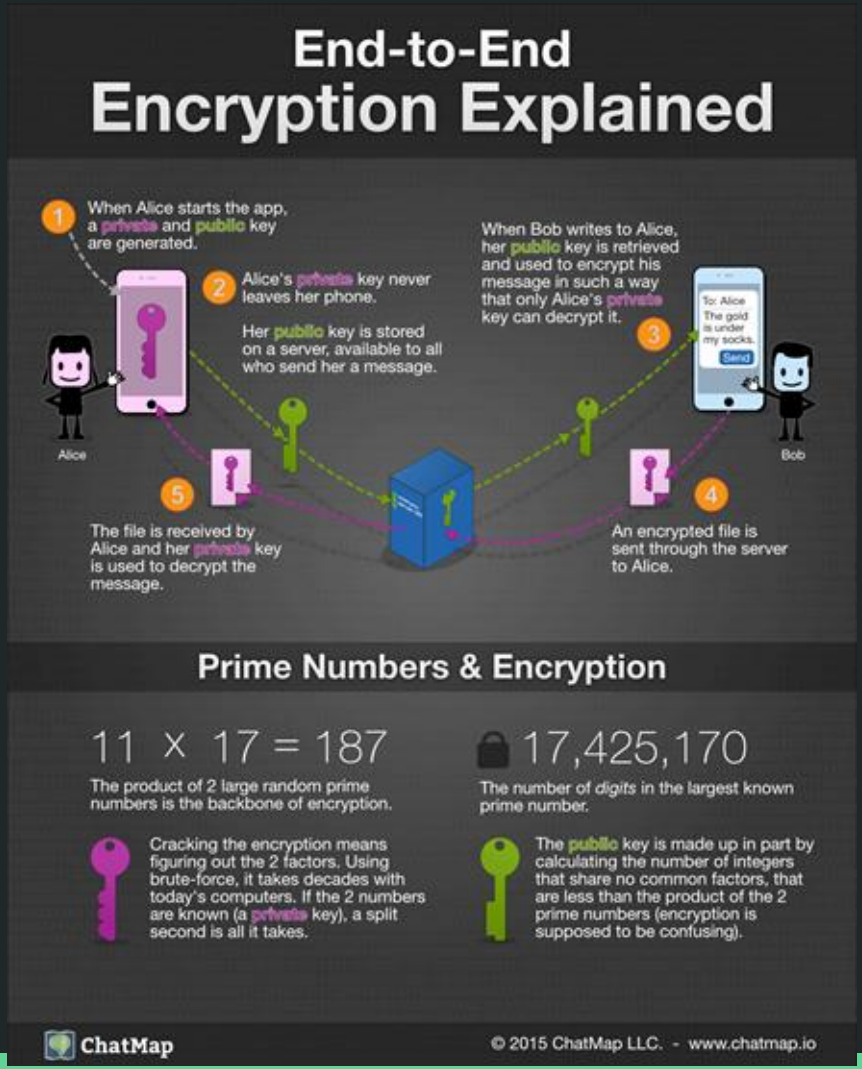
- commerce et protection de sites web → protocole SSL (Secure Sockets Layers ou Couche de transport sécurisé)

protocole en trois étapes:

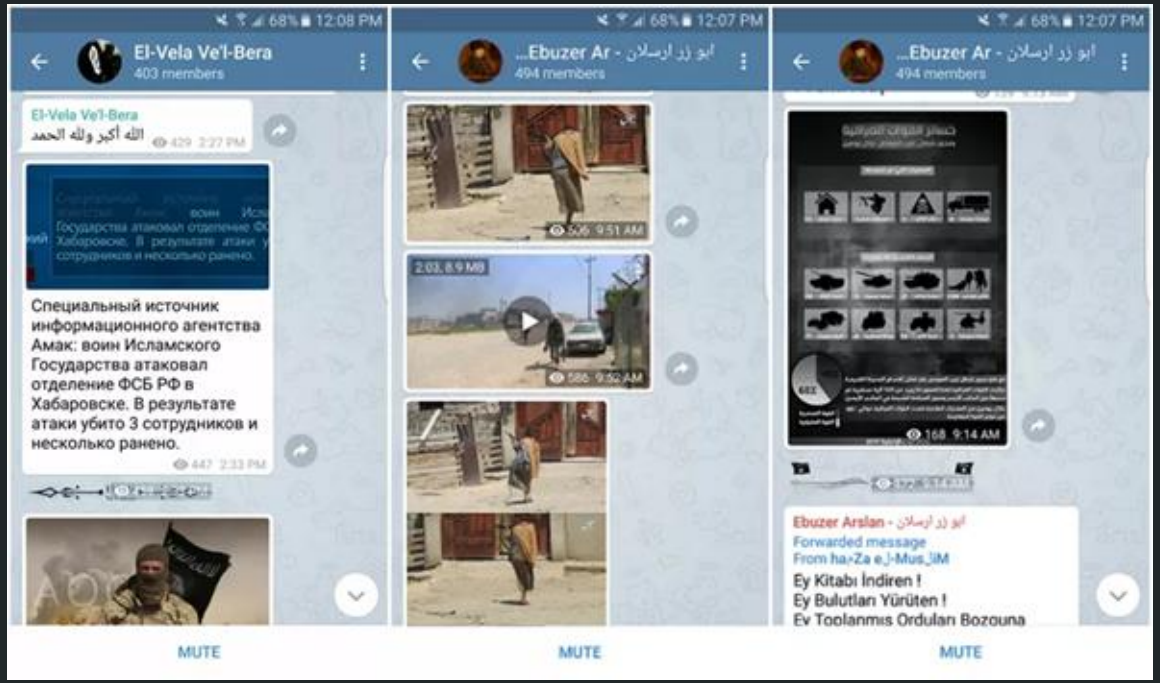
- authentification
- assurer la confidentialité
- préserver l’intégrité des données



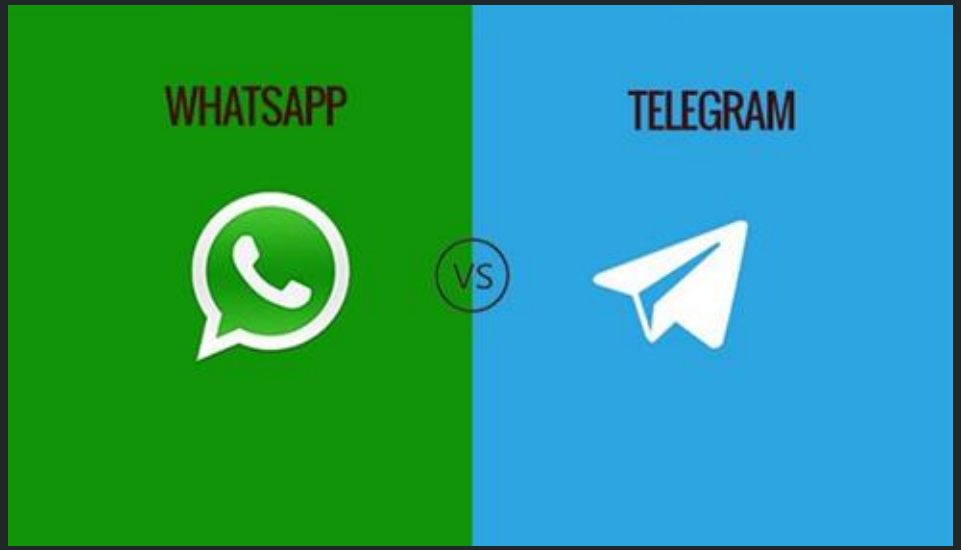
- communication → “end-to-end encryption”



Telegram et le terrorisme



WhatsApp vs Telegram



Crypto Contest Ends

The current round of our contest to crack Telegram's encryption ends with no winners. Despite the **$300,000** bounty and the fact that contestants could act as the Telegram server passing info between the users (i.e. use any kinds of active attacks, manipulate traffic etc.) no one could decipher their Secret Chats by the beginning of February.

To demonstrate that the contest was fair, we've added a decryption method to the contest bot's list of commands – **KEY**. **KEY** returns the 256-byte encryption key used in the secret chat, so the task of the contest is now easily achieved.

Why are contests important?

One of the reasons we trust Telegram's Secret Chats more than many of their alternatives, is that they're open to scrutiny from the world's security experts. And while having open source apps and a well documented API makes this kind of scrutiny possible, it is our contests that create incentive for it.

That's why we will definitely launch the next round of our contest later this year. It'll take us some time to determine whether we can further simplify the task for the contestants. Once ready, we'll announce the new round on Twitter.

Thank you for the vast amount of advice and comments you sent us during these last few months – your input allows us to improve Telegram with each new build.

February 11, 2015
The Telegram Team

L’avenir et débat de la cryptographie

- Cryptographie quantique

Sources

https://fr.wikipedia.org/wiki/Logiciels_de_cryptographie
http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/index
http://perso.telecom-paristech.fr/~guilley/enseignement/projets/crypto_ethique/compte_rendu_05nov02.php
http://perso.telecom-paristech.fr/~guilley/enseignement/projets/crypto_ethique/ethique_de_la_cryptologie.pdf
http://www.liberation.fr/sciences/2015/03/26/cryptographie-monde-cles_1228976
http://www.liberation.fr/futurs/2015/09/13/cryptographie-la-justice-cherche-la-cle_1381801
https://telegram.org/blog/cryptocontest-ends
https://www.tecmundo.com.br/mensageiros/75497-especialistas-hackeiam-telegram-criticam-encriptacao-horripilante.htm
https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter
https://www.forbes.com/sites/leonhardweese/2016/08/10/which-app-is-more-secure-telegram-or-whatsapp/#21946efb3cdf
http://neurogadget.net/2017/07/06/whatsapp-vs-telegram-which-app-is-more-secure/55430
https://www.expressvpn.com/blog/whatsapp-vs-telegram-encryption-battle/
http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/comelectro