T°S	SÉANCE DU VENDREDI 29 MAI 2020

Un chiffrement asymétrique : le protocole RSA (1976) : suite

On continue sur le chiffrement le plus connu au monde (le système « RSA »).
Rappel du lien de l'activité : https://www.mathemathieu.fr/component/attachments/download/286.

J'abrège vos souffrances : je ne vous demande que de **lire la page 4** (« le protocole RSA ») afin de comprendre comment ce génial protocole fonctionne.
Pour ceux que la suite de l'activité intéresse (je suis naïf), voici la correction :
https://www.mathemathieu.fr/component/attachments/download/1326

Ensuite, je vous encourage vivement et avec plein d'amour à en apprendre un peu plus sur comment est utilisé cet algorithme (ou ce genre de chiffrement asymétrique) en **regardant cette vidéo (≈ 20 min)** de Monsieur Bidouille : https://youtu.be/Fqvo6M2d5IQ. Vous y découvrirez des infos sur le protocole HTTPS que vous utilisez tous les jours sur Internet, la notion de signature numérique que vous utiliserez en payant vos impôts en ligne mais qui est aussi utilisé dès que vous êtes sur Internet, la notion d'empreinte (=« hash » : notion très importante que vous manipulez sans le savoir, entre autres, dès que vous copiez-collez un fichier sur un ordinateur ; quand vous accédez à mon site : les mots de passe ne sont pas enregistrés dans ma base de données, ce sont les « hash » qui le sont, ainsi même si on me pirate mon site, vos mots de passe sont protégés ; aussi très utilisé pour les cryptomonnaies), etc.

Ceci était notre dernière séance.
Si vous avez tout fait sérieusement, même pendant le confinement, vous pouvez être fier de vous : vous avez choisi la spécialité la plus difficile. Vous avez été courageux. Vous avez mon respect alors que les autres ne méritent que mes postillons et mon mépris. Vous êtes l'élite de la Nation, vous nous éviterez l'Apocalypse. Vous êtes le futur de la France.
(ça va, j'en fais pas trop ?)

Vive la pensée critique. Vive les (belles) mathématiques. Vive l'arithmétique.
Adieu.