

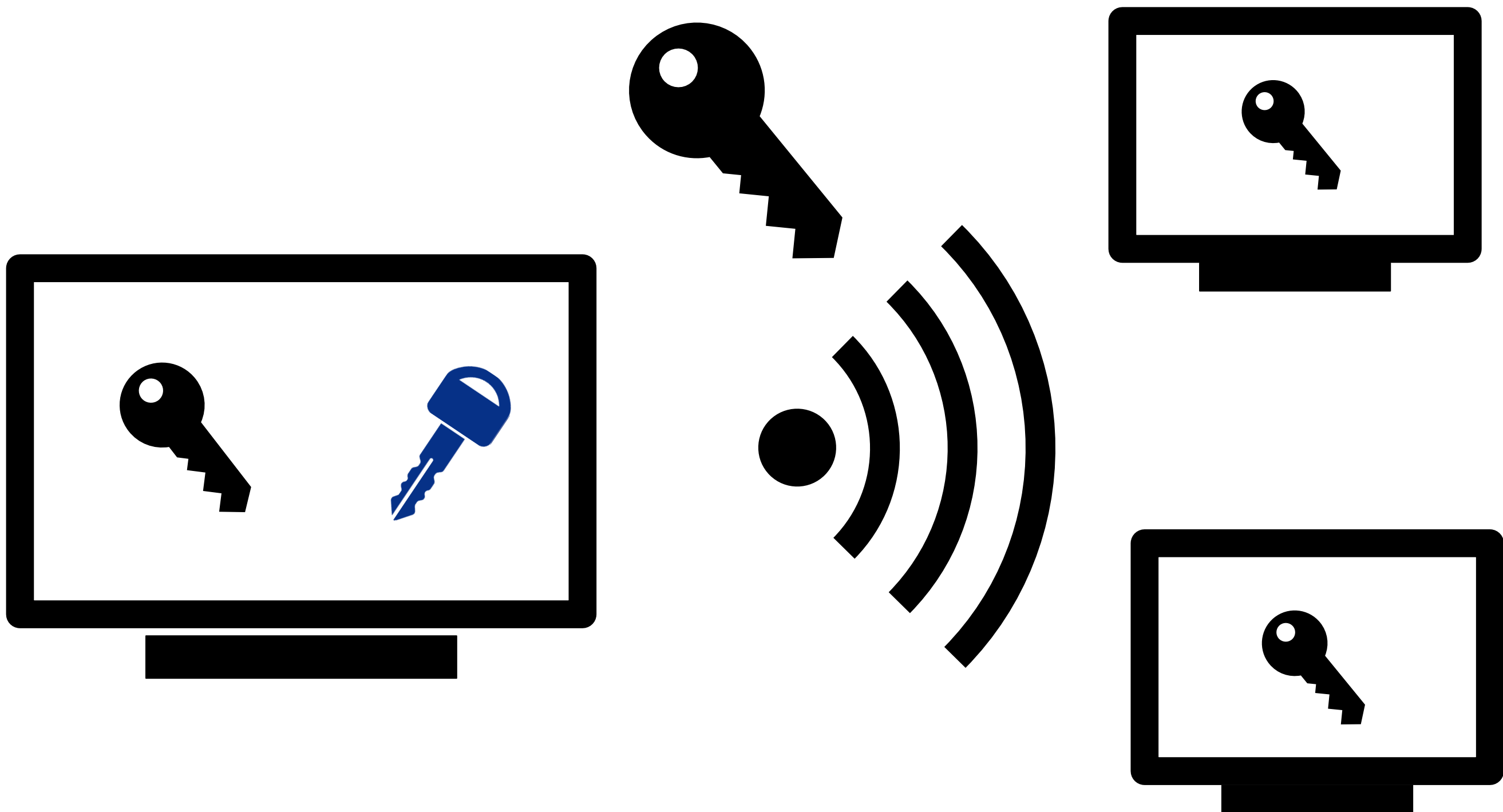
UNIVERSITÉ LIBRE DE BRUXELLES – FACULTÉ DES SCIENCES
DÉPARTEMENT D'INFORMATIQUE

David COPOT, Rares RADU-LOGHIN, Lucas VERBEIREN et Ethan VAN RUYSKENSVELDE

La Cryptographie Asymétrique

Des secrets basés sur les mathématiques

La cryptographie asymétrique joue un rôle majeur dans la communication sécurisée sur Internet. Contrairement aux méthodes classiques symétriques où une seule clé est partagée, ce système repose sur une paire de clés qui sont liées mathématiquement : la clé publique, que tout le monde peut connaître pour chiffrer un message, et la clé privée, que seul le destinataire possède pour le déchiffrer. Ce concept permet de garantir la confidentialité et l'authenticité des échanges sans jamais avoir à s'échanger de secret au préalable.



Clé publique : n, e : (12473100388834479437, 65537)
Clé privée : d : 12245285541945532673

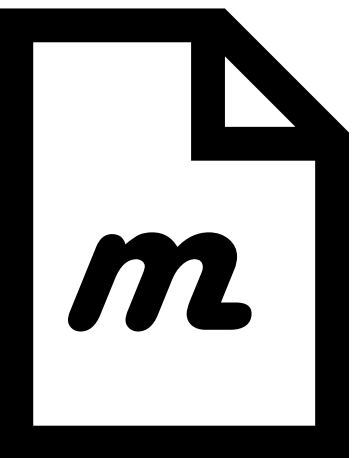
Chiffrement et envoie de messages

A vous de jouer

Nous vous invitons à participer à notre petit jeu de piste. En scannant le code QR ci-dessous, une clé publique et privée seront générée spécialement pour vous. La suite est simple : déchiffrez le message que nous vous enverrons et suivez les instructions.

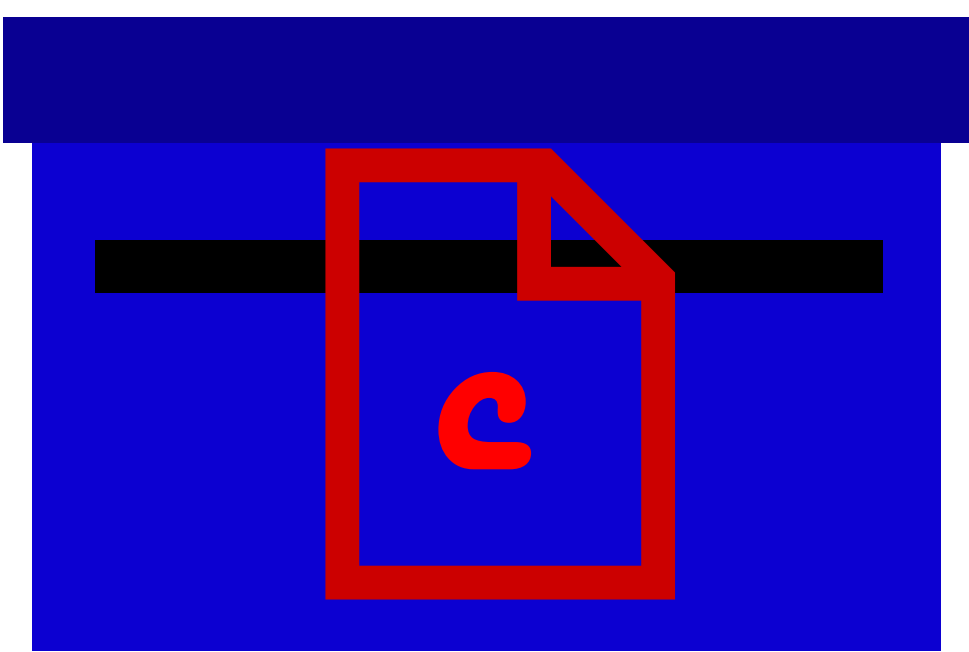


Choix de p et q
On choisit deux nombres premiers que nous appelons p et q
Calcul de n
$n = p \cdot q$
Calcul de $\varphi(n)$
$\begin{aligned}\varphi(n) &= \varphi(p \cdot q) \\ &= \varphi(p) \cdot \varphi(q) \quad (\text{car } p \text{ et } q \text{ sont copremiers}) \\ &= (p - 1)(q - 1) \quad (\text{car } p \text{ et } q \text{ sont premiers})\end{aligned}\tag{1}$
Choix de l'exposant publique e
$\begin{aligned}1 &< e < \varphi(n) \\ \text{pgcd}(\varphi(n), e) &= 1\end{aligned}$
Calcul de d , l'inverse modulaire de e
$d \equiv e^{-1} \pmod{\varphi(n)}\tag{2}$
Clé publique et privée
- Clé publique : (n, e) - Clé privée : d



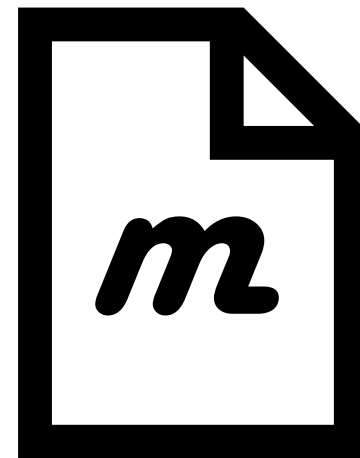
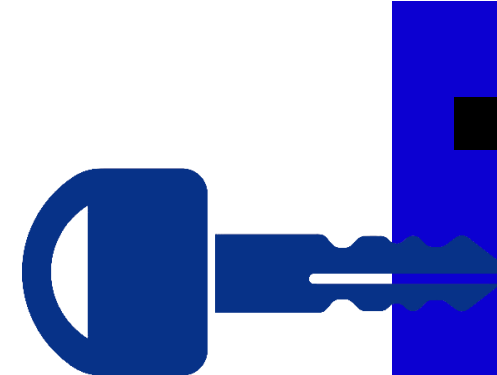
Une clé publique connue de tous

- La Clé Publique:** Elle est représentée par une boîte pouvant accepter des messages déposés par n'importe qui. Mettre un message dans la boîte est synonyme de le chiffrer.



Un message chiffré incompris de tous

- Le Message Chiffré:** Le message se trouve dans la boîte et ne peut être lu par personne tant qu'il s'y trouve.



Une clé privée restée cachée

La Clé Privée: Seul le propriétaire de la boîte aux lettres possède la clé unique permettant d'ouvrir l'ouvrir. Le fait d'ouvrir la boîte représente donc le déchiffrement.