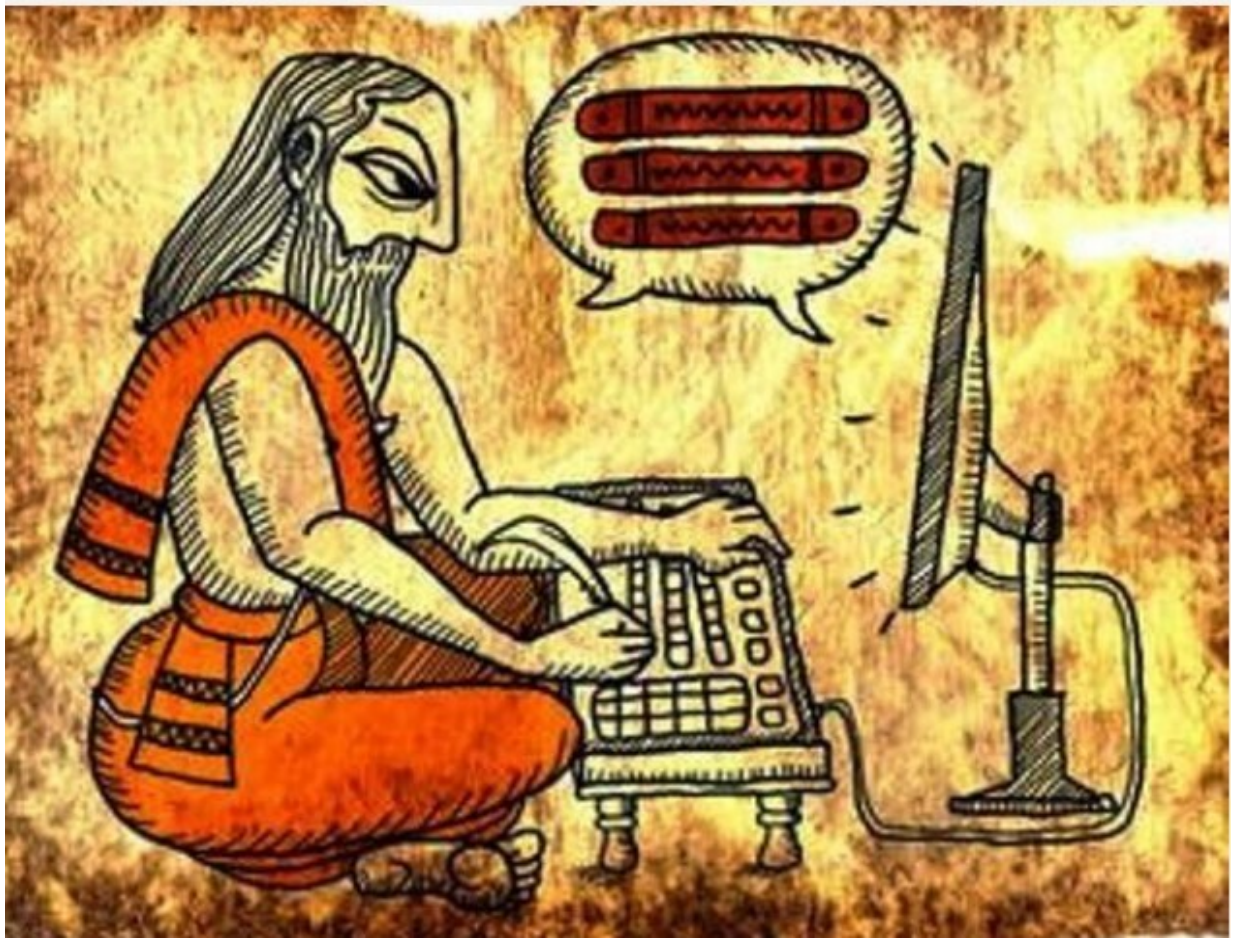
CRYPTOLOGIE

Un Peu d'ALGO



STARINUX

C J U P

(**C**haque **J**our **U**n **P**eu)

Référence :

Le CHIFFREMENT à CLEF PUBLIQUE et le RSA

21 décembre 2024 - 1 - Présentation

MAJ :

01/11/2024

► Ce document présente le sommaire de l'atelier du **21 décembre 2024**, programmé à l'association **STARINUX**, sur le thème de la **cryptographie à clé publique**, et en particulier sur le **RSA**.

► Titre de cet exposé :

« Le CHIFFREMENT à CLEF PUBLIQUE et le SYSTÈME RSA »

S O M M A I R E

1 **RAPPEL de QUELQUES OUTILS MATHÉMATIQUES**

PGCD, Algorithme d'Euclide et Théorème de Bézout
Congruence - Opérations d'Arithmétique Modulaire
Théorème de FERMAT - Tests de Primalité

2 **La RÉVOLUTION de la CRYPTOGRAPHIE PUBLIQUE**

Le Protocole de DIFFIE-HELLMANN (1976)

3 **Le SYSTÈME RSA**

Le Fonctionnement *théorique* du Système RSA (1978)

4 **EXERCICES d'APPLICATION**

Exercices de chiffrement
(tableurs CALC et GNUMERIC, logiciels OCTAVE, XCAS)

H O R A I R E

MATIN

9H30-9H45	**PRÉSENTATION**
9H45-11H00	**Les OUTILS MATHÉMATIQUES à CONNAÎTRE** PGCD et ALGORITHME d'EUCLIDE CONGRUENCE - OPÉRATIONS d'ARITHMÉTIQUE MODULAIRE TESTS de PRIMALITÉ (Fermat, Solovay-Strassen, Rabin-Miller)
11H00-11H30	**La NOTION de CLEF PUBLIQUE** Le Protocole de DIFFIE-HELLMANN (1976)
11H45-13H	**Le Système RSA** Le Fonctionnement *théorique* du Système RSA (1978)

APRÈS-MIDI

14H30-16H Pause 16h30-18h	Exercices de calcul et de (dé)chiffrement avec les outils logiciels CALC, GNUMERIC, OCTAVE et XCAS Discussion