

Sécurité Informatique



Composante
École Nationale
Supérieure
d'Électrotechnique
d'Électronique
d'Informatique
d'Hydraulique
et des
Télécommunications

En bref

> **Code:** N9EE20A

Présentation

Description

Introduction aux concepts de base de la sécurité des systèmes d'information (classification des attaques, cryptographie, évaluation)

Illustration par des exemples (DES/AES, RSA, Diffie-Hellmann, signatures électroniques)

Authentification et protocoles d'authentification sans apport de connaissance (Needham-Schroeder, Fiat-Shamir). Exemples : Kerberos, carte à puce.

Protection dans les systèmes informatiques (politique de sécurité discrétionnaire et obligatoire) et exemples

Notions de tolérance aux intrusions (schémas à seuil de Shamir, etc.).

Pré-requis obligatoires

Connaissances de base en informatique (matériel, système opératoire, langage)