Université de Bretagne Occidentale

FACULTÉ DES SCIENCES & TECHNIQUES

MASTER RÉSEAUX ET TÉLÉCOMMUNICATIONS

PARCOURS TÉLÉCOMMUNICATIONS, RÉSEAUX ET CYBERSÉCURITÉ

Semestre 7

Cryptographie et sécurité

Présentation

4 crédits ECTS

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 12h
Travaux Pratiques : 16h

La cryptographie est à la base de la sécurisation des transmissions. Connaître les principes de la cryptographie, les principaux algorithmes avec leurs forces et leurs faiblesses est indispensable au concepteur d'un système sécurisé.

Dans cette UE, nous donnons à l'étudiant une bonne connaissance des principes essentiels, une description des algorithmes importants, afin qu'il puisse choisir la méthode la plus adaptée à un contexte donné, en aillant une bonne compréhension de ses faiblesses potentielles.

Un accent particulier est également mis sur le chiffrement homomorphe qui permet de confier à un serveur un calcul complexe sans divulguer les données, et est donc par là-même appelé à connaître un essor important avec le développement du « cloud computing ».

Une sensibilisation à la vulnérabilité des principaux algorithmes actuels à une attaque par calculateur quantique terminera cet enseignement.

Objectifs

- Connaître les principes de la cryptographie et quelques algorithmes importants.
- Savoir choisir la méthode adaptée en fonction d'un cahier des charges.

Pré-requis nécessaires

Notions mathématiques : calcul modulaire, polynômes, vecteurs et matrices.

Compétences visées

- Algorithmes de chiffrement à clés secrètes et à clés publiques.
- Etude détaillée d'algorithmes: RC4, AES, RSA Fonctions de hachage.
- Signature cryptographique. Authentification.
- Déléguer un calcul sans divulguer ses données : chiffrement homomorphe.
- Distribution quantique des clés : exemple du réseau Chinois QUESS.
- Cryptosystèmes basés sur les codes correcteurs d'erreurs et sensibilisation à la cryptographie post-quantique (résistance à un attaquant disposant d'un calculateur quantique).

Bibliographie

Des références actualisées chaque année seront fournies en cours.

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CC	Ecrit - devoir surveillé		67%	
UE	CC	Travaux Pratiques		33%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé		100%	