Master Informatique
Cryptographie

Responsable

Remi MORIN
remi.morin@univ-amu.fr

Descriptions

Code : S51IN2A7

Nature :

Domaines : Sciences et Technologies

Informations

Composante : Faculté des Sciences

Nombre de crédits :

CONTENU

Cette UE propose un tour d'horizon de la cryptographie moderne: il s'agit d'initier les étudiants du Master Informatique aux problématiques fondamentales de **confidentialité**, d'**authentification** et d'**intégrité**, illustrées sur des cas concrets. Une attention particulière est portée sur la mise-en-oeuvre de primitives cryptographiques à l'aide de librairies spécifiques afin d'être en mesure d'incorporer des fonctionnalités cryptographiques dans un logiciel sécurisé.

Les différents types de solutions sont présentés: **chiffrements** symétrique, asymétrique, par flot, par blocs, ou hybride pour la confidentialité; les **fonctions de hachage** courantes et leurs applications à l'intégrité, au stockage des mots-de-passe, au chiffrement par mot-de-passe, ou à l'authentification non-interactive; les certificats, les autorités de confiance et les **trousseaux de clefs** pour la sécurité des protocoles.

Le détail de plusieurs fonctions considérées comme sûres, et recommandées par l'ANSSI, telles que l'AES, le RSA, le DSA font l'objet d'un codage complet en C ou en Java (au choix) afin de développer une expertise technique de base. En particulier, les Travaux Pratiques permettent de s'initier à l'utilisation de librairies standards pour le calcul sur de grands entiers, à savoir **GMP** en C ou **BigInteger** en Java. La phase de **bourrage**, dans l'AES ou le RSA, et l'emploi d'un mode opératoire sont également implémentés. Enfin, l'utilisation de l'API JCE (Java Cryptography Extension) ou de la librairie OPENSSL permet de consolider les connaissances et les savoir-faire acquis mais aussi d'explorer de nouvelles primitives.

Quelques protocoles d'**échange de clefs de session** et d'authentification interactive sont étudiés en fin de cours.

VOLUME HORAIRE

- Volume total: 27 heures

CODES APOGÉE

- SINBU03L [ELP]

M3C

Aucune donnée M3C trouvée

POUR PLUS D'INFORMATIONS

Aller sur le site de l'offre de formation...

Dernière modification le 19/03/2024