SYMMETRIC AND ASYMMETRIC CRYPTOLOGY ; PKI ARCHITECTURES [6 ECTS]

Cryptologie symétrique et asymétrique, Architectures PKI

Code ECTS

Course total volume: 60h
Period : 1 semester

Professors : Roland GILLARD, Philippe ELBAZ-VINCENT, Jean-Guillaume DUMAS

E-mail : roland.gillard@ujf-grenoble.fr, pev@fourier.ujf-grenoble.fr, jean-guillaume.dumas@imag.fr

Objectives :

Introduction to symmetric and asymmetric encryption and their use in public key architecture

Stream and block ciphers (Prof. R Gillard): review of the main systems; give some notions In analysis.

Public key methods (Prof. P Elbaz-Vincent): presentation of modern public key cryptography. The course will describe in details (including state of the art on their cryptanalysis) RSA, ECC.(and more generally DLP based cryptosystems) and NTRU and theirs associated protocols.

Public Key Infrastructure (Prof. JG Dumas): A Public Key Infrastructure is a set of infrastructures making it possible to carry out secure exchanges. Indeed, in a public key setting, the first practical problem is how to attach a public key to its owner? The idea of the PKI is initially not to distribute keys but rather numerical certificates containing these keys as well as identity data (status, mail, e-mail, domain name or IP addresses IP for a server...). The objectives of this course are to master the precise structures and tools ensuring in particular creation and management of these certificates. Several applications in secure Internet or protected electronic mail as well as the concepts of safety policy allowing a sensible management of these certificates are approached.

Contents

Stream and block ciphers : **I**ntroduction-Basic Facts, Data Encryption Standard, System Description ,Programing Attacks, Cryptanalysis ; Other Systems I (Variants : Lucifer, Gost, XDES, 3-DES). Idea, Blowfish. Advanced Encryption Standard, Other Systems II (Other AES candidates: Mars, 2fish,RC6,Serpent,CS, Misty/Kasumi, Camélia, SHACAL). Streamciphers : LFSR Massey-Berlekamp Algorithm Main systems Geffe,RC4,A5,PKZIP,Bluetooth Attacks. Comments.

Public key methods : An overview on cryptology2. Fundamental concepts, basic and advanced cryptanalysis, "real life" protocols (including semantic security) for the following public key cryptosystems: RSA, Diffie/Hellman and ElGamal (including ECC), NTRU.3. Overview on others public key cryptosystems

PKI*:* Introduction (Needs; What is public key infrastructure? Security Policy ? Context and theoretical background.. Infrastructures Principle , PKI Elements (PKI functions ; PKI entities) Certificates (emission ; PGP; X.509 ; Applications) Hierarchical PKI (PKIX Model ; Administration ; Authentification ; Migration) Non hierarchical PKI (PGP confidence, Spooky/Sudsy, ...) Drawbacks of PKI. Web Security, electronic mail and PKI. IPSEC ; SSL, TLS ; S/MIME ; DNSsec ; LDAP ; SET ; IKE. Security Policy and Infrastructures Security procedures ; Certification Policy ; Threat Modelling

Prerequisites :

Stream and block ciphers : Basic Algebra

Public key methods : knowledge of arithmetic over the intergers and modular arithmetics. Knowledge on finite fuelds. Undergraduate linear algebraand commutative algebra. Basic knowledge on probability and statistics. Basic knowledge on complexity theory and programming languageSome familiarity with at least one computational algebra system.

PKI **:** Secret key Cryptography, Public Key Cryptography, e-Signature, Hash functions

Continuous Examination :

Stream and block ciphers 2 practical works
Public key methods : 1 computer classroom evaluation and 1 classroom evaluation
PKI 1 assignment and 1 practical exam

1 final exam in 3 parts

Final mark session1: 20%*TP + 15%*CC + 65%*ET
Final mark session2: 20%*TP + 15%*CC + 65*ET2 (if ET2 >ET1)

DESCRIPTION IN FRENCH

Objectifs de l'enseignement :

Cryptographie symétrique **:** Présentation des systèmes principaux avec quelques notions d'analyse

Méthodes de cryptologie à clef publique : Le cours décrira en détails (y inclus un état de l'art sur leurs cryptanalyses) RSA, ECC (et plus généralement les méthodes basées sur le DLP) et NTRU, ainsi que les protocoles associes

PKI : Une architecture PKI (pour Public Key Infrastructure) est un ensemble d'infrastructures permettant de réaliser effectivement des échanges sécurisés. En effet, une fois définis des algorithmes complexes utilisant par exemple des clefs publiques, le premier problème pratique qui se pose est comment rattacher une clef publique à son propriétaire? L'idée des PKI est d'abord de ne pas distribuer des clefs mais plutôt des certificats numériques contenant ces clefs ainsi que des données d'identité (état civil, adresse, adresse mail pour une personne, nom de domaine ou adresse IP pour un serveur...). L'objectif de ce cours est de maitriser les structures précises et les outils assurant en particulier la création et la gestion de ces certificats au sein par exemple d'une entreprise. De nombreuses applications en sécurité internet, messagerie électronique sécurisée ainsi que des notions de politique de sécurité permettant la gestion raisonnée de ces certificats sont abordées

Contenu :

Cryptographie symétrique : Introduction-Généralités, Data Encryption Standard, Description du systèmeProgrammation, Attaques, Cryptanalyse Autres Systèmes I (Variantes : Lucifer, Gost, XDES, 3-DESIdea, Blowfish). Advanced Encryption Standard , Autres Systèmes II (Autres candidats AES : Mars, 2fish,RC6,Serpent , CS, Misty/Kasumi, Camélia, SHACAL). Systèmes par flot (LFSR , combinaison, flitrage , Algorithme de Massey-Berlekamp).Principaux systèmes : Geffe,RC4,A5,PKZIP,Bluetooth. Attaques Discussion et Remarques finales Blocs et flots, Blocs et fonctions de hachage
Presentation des methodes modernes de cryptogrphie a clefs publiques.

Méthodes de cryptologie à clef publique :. Un panorama de la cryptologie.. Concepts fondamentaux, cryptanalyses elementaires et avances, protocoles (y inclut preuve de securite semantique) pour les cryptosystemes a clefs publiques suivants ; RSA, Diffie/Hellman et ElGamal (y inclut ECC), NTRU.. Presentation d'autres cryptosystemes a clefs publiques

PKI : Introduction et contexte (Qu'est-ce que la PKI ? ; Signatures électroniques)..
Éléments d'une infrastructure PKI (Fonctions et acteurs d'une PKI : CA, RA, Dépôt, etc.) * Les certificats (Émission et vérification d'un certificat, PGP, un premier exemple de certificat, Certificats X.509, exemples dans Mozilla, Windows XP, etc.)P KI hiérarchiques (PKIX, Les fonctions d'administration, Authentification, Migration). Architectures non hiérarchiques (Modèle de confiance PGP, Spooky/Sudsy, ...) Défauts des PKI. OpenSSL : mise en place d'une PKI d'entreprise Protocoles de Sécurité Web et courrier électronique. Couche réseau : IPSEC ; Couche transport : OpenSSL, TLS ; Couche applicative (S/MIME, DNSsec, LDAP, PGP et GnuPG, SET, e-carte bleue). Politiques et Architectures de Sécurité. Mesures de sécurité ; Politique de certification ; Modélisation de la menace ; Aspects légaux

Pré requis :

Cryptographie symétrique : algèbre de base
Méthodes de cryptologie à clef publique : .Connaissance de l'arithmétique des entiers et de l'arithmétique modulaire. Manipulations des corps finis. Algèbre et algèbre linéaire de Licence. Rudiments de théorie des probabilités et de statistiques. Connaissance de base en théorie de la complexité et en langages de programmation.
Connaissance d'au moins un logiciel de calcul formel.
PKI **:** Cryptographie à clef secrète, Cryptographie à Clef publique, Signature Electronique, Fonctions de Hachage

Contrôle continu :
Cryptographie symétrique : **2** TP, un examen terminal
Méthodes de cryptologie à clef publique : 1 travaux pratiques noté ,1 contrôle continu en classe1 examen final
PKI Contrôle continu, 1 TP

Contrôle final : en 3 parties

Bibliographies / textbooks

- Bruce Schneier : Applied Cryptography
- A.J. Menezes, P.C. van Oorshot, S.A. Vanstone : Handbook of Applied cryptography, CRC Press 1997
- D. Stinson : Cryptography, theory et pratique, .Int. Thomson Pub France 1996. et 2nd éd 2003.
- S. Vaudenay A classical Introduction to Cryptography , Applications for COmmunications Security, Springer 2006
- Mao, W; Modern Cryptography: Theory and Practice, 2003
- Hankerson, D; Menezes, A; Vanstone, S; Guide to Elliptic Curve Cryptography 2004
- Koblitz, N; Algebraic Aspects of Cryptography 2004
- Yan, S; Primality Testing and Integer Factorization in Public-Key Cryptography, 2003
- Yan, S; Cryptanalytic Attacks on RSA , 2007
- Carlisle Adams and Steve Lloyd. Understanding PKI: Concepts, Standards, and Deployment Considerations. Addison-Wesley Professional; 2nd edition 2002.
- C. Cachat et D. Carella. PKI Open source : déploiement et administration. O'Reilly 2003.
- Cryptographie et sécurité des systèmes et réseaux, T. Ebrahimi, F. Leprevost, and B. Warusfeld, éditeurs, Hermès 2006.
- J-G. Dumas, J-L. Roch, É. Tannier et S. Varrette. Théorie des codes : compression, cryptage, correction. Dunod 2007.
- B. Schneier. Secrets et Mensonges : sécurité numérique en réseau. Vuibert Informatique 2001.