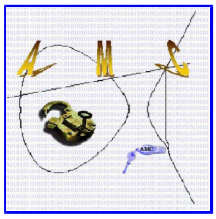
جامعة محمد الخامس السويسي
المدرسة الوطنية العليا للمعلوماتية و تحليل النظم

Université Mohammed V- Souissi
Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes



L'Association Marocaine de Cryptographie

REFERENTIELS DE LA CRYPTOGRAPHIE MODERNE

Du Mardi 28 au Vendredi 31 octobre 2008

A l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS)

Programme

Horaires	9h – 10h30		10h45 – 12h15		14h30– 16h		16h30 – 18h
Mardi 28 octobre 2008	**A. AZHARI** Tutoriel de la cryptographie moderne Partie I	Pause Café	**A. AZHARI** Tutoriel de la cryptographie moderne Partie I	Déjeuner	**A. AZHARI** La cryptographie en droit marocain et droit comparé	Pause Café	**A. NITAJ** **Atelier** Crypter et décrypter en MAPLE
Mercredi 29 octobre 2008	**A. NITAJ** **Cours** Introduction aux courbes elliptiques	Pause Café	**A. ENGE** **Cours** Couplage sur les courbes elliptiques Partie I	Déjeuner	**A. ENGE** **Cours** Couplage sur les courbes elliptiques Partie II	Pause Café	**A. AZHARI** **Exposé** IBE–COCKS
Jeudi 30 OCTOBRE 2008	**G. HANROT** **Cours** Arithmetique pour la cryptologie Partie I	Pause Café	**G. HANROT** **Cours** Arithmetique pour la cryptologie Partie II	Déjeuner	**A. NITAJ** **Cours** Les courbes elliptiques et les systèmes de calcul	Pause Café	**A. ENGE** **Exposé** Construction de courbes elliptiques pour la cryptographie
Vendredi 31 octobre 2008	**G. HANROT** **Cours** Arithmetique pour la cryptologie Partie III	Pause Café	**A. ENGE** **Cours** Couplage sur les courbes elliptiques Partie III	Déjeuner	**M. HEDABOU** **Exposé** IBE-BONEH & FRANKLIN	Pause Café	**G. HANROT** **Exposé** Réduction des réseaux

Liste des orateurs

Andreas Enge : Ecole Polytechnique, Palaiseau, France

Guillaume Hanrot : INRIA, LORIA, NANCY, France

Abdelhak Azhari : Université de Casabalanca, Maroc

Mustapha Hedabou : INSA, Toulouse, France

Abderrahmane Nitaj : LMNO, Caen, France

Contact

Abdelhak Azhari

Email: aazhari@amcrypto.org