INTITULE DE LA MATIERE : Sécurité Matérielle

CODE : SEMESTRE : 9

NOM DE L'ENSEIGNANT RESPONSABLE :

NOMBRE D'HEURES ENCADREES CM : 12 TD : TP :

NOMBRE D'HEURES DE TRAVAIL PERSONNEL DE L'ELEVE – estimation :

OBJECTIF GENERAL (pas plus de 10lignes) :

Présentation de standards cryptographiques asymétriques (RSA, El Gamal, chiffrement sur courbes elliptiques) et symétriques (AES), ainsi que de compactage de données (SHA1, SHA2, SHA3, SHA256). Différentes cibles : processeurs sécurisés, cartes à puce, lecteurs de cartes. Exemples d'implantations logicielles mais surtout matérielles de ces algorithmes. Attaques et contre-mesures. Notions de cryptographie quantique.

CONTENU – PLAN DU COURS (pas plus de 15 lignes) :

Présentation de différents domaines nécessitant l'implantation d'éléments de sécurité. Algorithmes de compactage de données (Secure Hash Algorithm) et ses différentes variantes SHA1, SHA2, SHA3, SHA256) et d'authentification (vérification de signature).

Définition de la cryptographie asymétrique ou à clé publique. Présentation des algorithmes Rivest Shamir Adleman (RSA), système d'El Gamal, cryptographie sur courbes elliptiques. Définition de la cryptographie symétrique ou à clé secrète. Présentation de l'algorithme Advanced Encryption Standard (AES). Comparaison des implantations logicielles et matérielles de standards cryptographiques. Exemple de réalisations de circuits dédiés à la sécurité (architectures, performances, prix). Attaques par analyse de consommation (SPA, DPA), attaque laser. Contre-mesures. Notions de cryptographie quantique.

FORME DE L'EVALUATION :

☐ Contrôle continu ☐ Contrôle terminal ☐ Mémoire/rapport ☐ Soutenance
préciser si nécessaire, nombre d'épreuves : et type oral / écrit

ACQUIS DE LA FORMATION ATTENDUS, ET QUI SONT EVALUES (5 à 10 items)

Avoir une revue de l'étendue du domaine de la cryptographie, des standards les plus utilisées, et avoir étudié des exemples d'implantation matérielle et optimisée de ces standards.

PREREQUIS (pas plus de 5 lignes):

REFERENCES, BIBLIOGRAPHIE (pas plus de 5 lignes) :