EN.09	***SECURISATION DES COMMUNICATIONS DES TECHNOLOGIES MINIATURISEES EMERGENTES***

Objectifs :

- *Familiarisation avec quelques technologies émergentes et apport de quelques connaissances théoriques et pratiques sur l'aspect sécurité et le respect de la vie privée ;*
- *Inculquer les techniques de cryptanalyse et d'authentification à base de la cryptographie par courbes elliptiques et les fonctions à sens unique ultralégères.*

Public concerné		***Pré-requis***			
Ingénieurs et plus		*Cryptographie, Algèbre, mathématiques*			
Niveau	***Session (s)***	***Durée***	***Début***	***Fin***	***Volume horaire***
II	*2*	*03 jours*	*09h*	*16h*	*18 heures*

Répartition du volume horaire

12 de Cours ; 6h de TP

Contenu du programme

I. THEORIE

I.1. Généralités sur la sécurité des systèmes miniaturisés

- *Technologies émergentes.*
- *Technologies RFID et ses limitations.*
- *La cryptographie légère et ultralégère.*
- *La cryptographie à base des courbes elliptiques.*
- *Services de sécurité offerts par la cryptographie.*
- *Authentification et confidentialité.*
- *Protocoles d'authentification.*

I.2. Attaques sur les systèmes miniaturisés

- *Attaques conventionnelles sur les schémas d'authentification.*
- *Exemple d'attaques sur les systèmes RFID.*

II. PRATIQUE :

- *Mise en œuvre des procédures d'identification sur un kit RFID réel.*
- *Mise en œuvre de quelques attaques conventionnelles sur des problèmes calculatoires.*

Enseignant (s) responsable (s) du stage	***Coût du stage (en H.T.)***
M. Mustapha BENSSALAH *M. Said SADOUDI*	60 000 DA