

Fonctions de hachage

Parties		Etudiant
Introduction, Definition, Motivations, Conclusion		MILENE
Fonctions de hachage cryptographique	Proprietes classiques et extenseur Merkle-Damgard	DOBA
	Extenseur eponge	DJOKAM
	Fonction MD5	DELYAN
	Fonction SHA-2	DOBA
Cryptanalyse des fonctions de hachage (attaque)		IVAN

Signatures numeriques

Parties	Etudiant
Introduction, Motivations, conclusion	CALVIN
Principe de base de la crypto asymétrique + PKI	ANDY
Schema RSA	MILENE
Schema DSA	DJOKAM
Schema ECDSA	IVAN
Schema Crystals-Dilithium ou ML-DSA	DELYAN
Limites et menaces	ANDY