R3.09 Cryptographie et sécurité -Partie maths

Informatique IUT de Saint-Dié-des Vosges



R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

### Programme

L'objectif de cette ressource est d'introduire les diverses techniques employées en cryptographie.

R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

### Programme

L'objectif de cette ressource est d'introduire les diverses techniques employées en cryptographie.

**1** Arithmétique  $(\mathbb{Z}/n\mathbb{Z})$ 

R3.09 Cryptographie et sécurité -Partie maths

Départemen Informatique IUT de Saint-Dié-des Vosges

### Programme

L'objectif de cette ressource est d'introduire les diverses techniques employées en cryptographie.

- **1** Arithmétique  $(\mathbb{Z}/n\mathbb{Z})$
- 2 Introduction à la cryptographie symétrique (César, Vigenère, Hill)

R3.09 Cryptographie et sécurité -Partie maths

Départemen Informatique IUT de Saint-Dié-des Vosges

### Programme

L'objectif de cette ressource est d'introduire les diverses techniques employées en cryptographie.

- **1** Arithmétique  $(\mathbb{Z}/n\mathbb{Z})$
- 2 Introduction à la cryptographie symétrique (César, Vigenère, Hill)
- 3 Cryptographie asymétrique (RSA)

R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

$$4 \text{ TD} + 5 \text{ TP (dont 1 TD} + 2 \text{ TP SAE)}$$

R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

### 4 TD + 5 TP (dont 1 TD + 2 TP SAE)

 SAE : Cryptanalyse de RSA - Fractions continues - Méthode de Wiener

R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

### 4 TD + 5 TP (dont 1 TD + 2 TP SAE)

- SAE : Cryptanalyse de RSA Fractions continues Méthode de Wiener
- TP ressources :
  - TP1 : Cryptographie asymétrique Cryptanalyse RSA
  - TP2: Cryptographie symétrique César, Vigenère, Hill -Chiffrement affine

R3.09 Cryptographie et sécurité -Partie maths

Départemen Informatique IUT de Saint-Dié-des Vosges



R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges



R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

### Ressources : Arche

- Cours
- QCM auto-formation : auto-test

R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

#### Ressources: Arche

- Cours
- QCM auto-formation : auto-test
- TD

R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

#### Ressources: Arche

- Cours
- QCM auto-formation : auto-test
- TD
- Documents de référence : LibreOffice, Maple

R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

### Ressources : Arche

- Cours
- QCM auto-formation : auto-test
- TD
- Ocuments de référence : LibreOffice, Maple Formulaire d'analyse

R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

### Ressources : Arche

- Cours
- QCM auto-formation : auto-test
- TD
- Documents de référence : LibreOffice, Maple Formulaire d'analyse
- Forum si besoin

R3.09 Cryptographie et sécurité -Partie maths

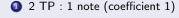
Informatique
IUT de
Saint-Dié-des
Vosges



R3.09 Cryptographie et sécurité -Partie maths

Departemen Informatique IUT de Saint-Dié-des Vosges

### Évaluations



R3.09 Cryptographie et sécurité -Partie maths

Département Informatique IUT de Saint-Dié-des Vosges

### Évaluations

1 2 TP : 1 note (coefficient 1) pm TP partie informatique : coefficient 1

R3.09 Cryptographie et sécurité -Partie maths

Départemen Informatique IUT de Saint-Dié-de Vosges

### Évaluations

- ① 2 TP : 1 note (coefficient 1) pm TP partie informatique : coefficient 1
- 2 1 devoir sur table (coefficient 2)

Ressources autorisés : documents distribués, cours, notes manuscrites et calculatrice.

R3.09 Cryptographie et sécurité -Partie maths

Départemen Informatique IUT de Saint-Dié-des Vosges

### Évaluations

- 2 TP : 1 note (coefficient 1) pm TP partie informatique : coefficient 1
- 2 1 devoir sur table (coefficient 2)
  Ressources autorisés : documents distribués, cours, notes manuscrites et calculatrice.
- 3 Évaluation du module