A R C S I - commission jeunes

Association des Réservistes du Chiffre et de la Sécurité de l'Information
Association « Loi 1901 » créée en 1928, reconnue d'intérêt général
N° SIRET : 511 069 569 00032

FICHE PÉDAGOGIQUE
OUTILS DE CHIFFREMENT - COMMISSION JEUNES ARCSI
Nom de l'outil : [PLAYFAIR]

Nom de l'outil : Chiffrement Playfair
Niveau de difficulté : Intermédiaire
Durée de l'activité : 30 à 45 minutes
Nombre de participants : 4-20 personnes
Public cible : Adolescents, étudiants, amateurs de cryptographie
Coût estimé : Coûts variables (matériel papier, stylos)
Logistique : Tables, chaises, tableau blanc, feutres

MATÉRIEL NÉCESSAIRE

- Papier et stylos pour chaque participant
- Tableau blanc ou paperboard
- Feutres
- Grille de chiffrement (imprimée ou dessinée à la main)

OBJECTIFS PÉDAGOGIQUES

- Comprendre le principe du chiffre de Playfair
- Apprendre à construire une grille de chiffrement
- Maîtriser la méthode de chiffrement et de déchiffrement avec la grille
- Découvrir l'histoire et l'utilisation des chiffrements classiques

MODE D'EMPLOI

1. **Préparation :**
   - Présenter le contexte historique du chiffre de Playfair
   - Expliquer la construction de la grille de chiffrement avec la clé donnée
2. **Utilisation :**
   - Distribuer la grille et expliquer la méthode de chiffrement
   - Montrer comment diviser un message en paires, gérer les doublons et lettres seules
3. **Méthode de chiffrement :**
   - Appliquer les règles (même ligne, même colonne, rectangle) pour chiffrer chaque paire
4. **Méthode de déchiffrement :**
   - Revenir à l'inverse des règles pour retrouver le message original

SCÉNARIO D'ANIMATION

Introduction (5 min)

- Présenter brièvement l'histoire du chiffre de Playfair
- Expliquer l'intérêt des chiffrements classiques dans la cryptographie

Démonstration (10 min)

- Construire la grille avec la clé « ARCSI »
- Chiffrer un exemple simple en direct (par exemple : "BONNE ANNEE")
- Montrer étape par étape le processus

Mise en pratique (15-20 min)

- Proposer aux participants de chiffrer leur propre message
- Vérifier la compréhension en déchiffrant un message chiffré fourni

---

Mise en pratique détail : Exercices progressifs à proposer

1. **Chiffrement d'un message simple :**
   - Demandez aux participants de chiffrer le message **"BONNE ANNÉE"** en utilisant la grille de Playfair construite avec la clé « ARCSI ».
   - Rappeler la procédure : diviser en paires, gérer les doublons, ajouter un X si nécessaire, puis appliquer les règles de chiffrement.
2. **Étapes détaillées pour le message « Bonne année » :**
   - **Division en paires :** BO, NN, EA, NN, EE
   - **Gestion des doublons et lettres seules :**
     - NN devient NX (pour éviter la double lettre)
     - La dernière lettre E seule devient EX
     - Message final à chiffrer : **BO NX NE AN NE EX**
3. **Chiffrement de chaque paire :**
   - **BO :**
     - B (ligne 2, colonne 1) et O (ligne 4, colonne 1)
     - Même colonne → remplacer par la lettre en dessous :
       - B → H (ligne 3, colonne 1)
       - O → V (ligne 5, colonne 1)
     - **Résultat : HV**
   - **NX :**
     - N (ligne 5, colonne 3) et X (ligne 3, colonne 5)
     - Forme un rectangle → remplacer par les lettres dans le coin opposé :
       - N → L (ligne 3, colonne 3)
       - X → Z (ligne 5, colonne 5)
     - **Résultat : LZ**
   - **NE :**
     - N (ligne 5, colonne 3) et E (ligne 2, colonne 3)
     - Forme un rectangle → remplacer par :

        - N → G (ligne 5, colonne 2)
        - E → L (ligne 3, colonne 3)
      - **Résultat : GL**
  - **AN :**
    - A (ligne 1, colonne 1) et N (ligne 5, colonne 3)
    - Forme un rectangle → remplacer par :
      - A → I (ligne 1, colonne 5)
      - N → H (ligne 1, colonne 3)
    - **Résultat : IH**
  - **NE (encore) :**
    - N (ligne 3, colonne 5) et E (ligne 2, colonne 3)
    - Rectangle → remplacer par :
      - N → G (ligne 5, colonne 2)
      - E → L (ligne 3, colonne 3)
    - **Résultat : GL**
  - **EX :**
    - E (ligne 2, colonne 3) et X (ligne 3, colonne 5)
    - Colonne → remplacer par la lettre en dessous :
      - E → L (ligne 3, colonne 3)
      - X → C (ligne 3, colonne 1)
    - **Résultat : LC**
4. **Message chiffré final :**
   HV LZ GL IH GL LC

Points d'attention

- Vérifier que les participants respectent la gestion des doublons et des lettres seules.
- Insister sur l'application correcte des règles selon la position des lettres dans la grille.
- Encourager à faire des exercices avec différents messages pour maîtriser la méthode.

Conclusion (5 min)

- Poser des questions pour vérifier la compréhension
- Discuter de l'évolution des méthodes de cryptographie et leur importance en cybersécurité

CONSEILS POUR L'ANIMATEUR

- Insister sur la logique des règles et leur application concrète

- Préparer des exemples variés pour illustrer chaque règle
- Adapter la difficulté selon le public (exemples plus ou moins complexes)
- Encourager la participation active pour mieux assimiler la méthode

POUR ALLER PLUS LOIN

- Références : Histoire de la cryptographie, autres chiffrements classiques
- Activités : Créer ses propres grilles, chiffrer des messages secrets
- Ressources en ligne : Tutoriels interactifs, générateurs de grilles

CONTEXTE HISTORIQUE

Le chiffre de Playfair a été inventé par Charles Wheatstone en 1854 et popularisé par Lord Playfair. Il s'agit d'un chiffre de substitution par digrammes, utilisé notamment dans la cryptographie militaire et diplomatique. Son principe repose sur une grille de 5x5, permettant une substitution plus complexe que le chiffre de César ou de substitution simple.