

Présentation de l'application de cryptographie

Rapport - Documentation



Introduction

Ce rapport présente une vue d'ensemble de l'Application de Cryptographie, une puissante solution pour sécuriser et gérer les données sensibles. L'application offre un large éventail de fonctionnalités, notamment le chiffrement, le déchiffrement, le hachage, la signature et la gestion des clés. Il sert de guide pour les utilisateurs, expliquant comment utiliser efficacement chaque fonctionnalité de l'application.

Fonctionnalités Principales :

-
- **Chiffrement et Déchiffrement** : Protégez vos données en chiffrant des messages ou des fichiers, puis déchiffrez-les lorsque vous en avez besoin.
 - **Hachage** : Créez des empreintes numériques uniques de vos données pour garantir leur intégrité.
 - **Signature** : Apposez des signatures numériques pour vérifier l'authenticité de vos documents.
 - **Message Authentication Code ou MAC** : Créez des empreintes numériques uniques de vos données pour garantir l'intégrité et la non répudiation en utilisant une clé secrète.
 - **Gestion d'algorithmes** : Choisissez parmi une variété d'algorithmes pour personnaliser votre sécurité.
 - **Génération de Clés** : Générez des clés sécurisées pour vos opérations de chiffrement et de signature.
 - **Gestion de Fichiers** : Stockez et gérez vos clés en toute sécurité pour des opérations ultérieures.

Cette documentation vous fournira des instructions détaillées sur la manière d'utiliser chaque fonctionnalité de l'application. Suivez les guides étape par étape pour tirer le meilleur parti de ces outils de cryptographie. Sécurisez vos données et assurez-vous de leur authenticité grâce à notre application de cryptographie.

Nous vous souhaitons une expérience sécurisée et productive avec notre application !

1. Création de compte et connexion

- **Création de compte**

La page de création de compte est l'endroit où les utilisateurs peuvent s'inscrire pour accéder à l'application.

L'utilisateur doit entrer les informations suivantes :

-
1. Prenom
 2. Nom
 3. Email
 4. Mot de passe

The screenshot shows a 'Creation Compte' form with a blue header bar. The title 'Creation Compte' is on the left, and a 'Se connecter' button is on the right. The form contains four input fields: 'Prenom' (with placeholder text 'Prenom'), 'Nom' (with placeholder text 'Nom'), 'Email' (containing 'massamba@gmail.com'), and 'Mot de passe' (with masked characters '.....'). A 'Creation' button is located at the bottom left of the form area.

- **Connexion**

La page de connexion permet à l'utilisateur d'accéder à son compte de pouvoir accéder aux fonctionnalités de l'application.

The screenshot shows a 'Connexion' form with a blue header bar. The title 'Connexion' is on the left, and a 'Creer un Compte' button is on the right. The form contains two input fields: 'Email' (containing 'massamba@gmail.com') and 'Mot de passe' (with masked characters '.....'). A 'Connexion' button is located at the bottom left of the form area.

2. La documentation

L'application est accompagnée d'une documentation complète directement intégrée pour faciliter l'utilisation et la compréhension de toutes ses fonctionnalités. Cette documentation a été conçue pour guider nos utilisateurs, qu'ils soient novices ou experts en matière de cryptographie, à travers les différentes étapes de l'application.

Documentation de l'Application de Cryptographie

Bienvenue dans la documentation de notre application de cryptographie ! Cette application vous offre un ensemble d'outils puissants pour sécuriser et gérer vos données sensibles. Vous pouvez effectuer diverses opérations, notamment le chiffrement, le déchiffrement, le hachage, la signature et la gestion de clés. Cette documentation vous guidera à travers les fonctionnalités de l'application et vous expliquera comment les utiliser de manière efficace.

Fonctionnalités Principales :

- **Chiffrement et Déchiffrement :** Protégez vos données en chiffrant des messages ou des fichiers, puis déchiffrez-les lorsque vous en avez besoin.
- **Hachage :** Créez des empreintes numériques uniques de vos données pour garantir leur intégrité.
- **Signature :** Apposez des signatures numériques pour vérifier l'authenticité de vos documents.
- **Gestion d'Algorithmes :** Choisissez parmi une variété d'algorithmes pour personnaliser votre sécurité.
- **Génération de Clés :** Générez des clés sécurisées pour vos opérations de chiffrement et de signature.
- **Gestion de Fichiers :** Stockez et gérez vos clés en toute sécurité pour des opérations ultérieures.

Cette documentation vous fournira des instructions détaillées sur la manière d'utiliser chaque fonctionnalité de l'application. Suivez les guides étape par étape pour tirer le meilleur parti de ces outils de cryptographie. Sécurisez vos données et assurez-vous de leur authenticité grâce à notre application de cryptographie.

Nous vous souhaitons une expérience sécurisée et productive avec notre application !

Algorithme Et Generation De Cle

Gestion d'Algorithmes

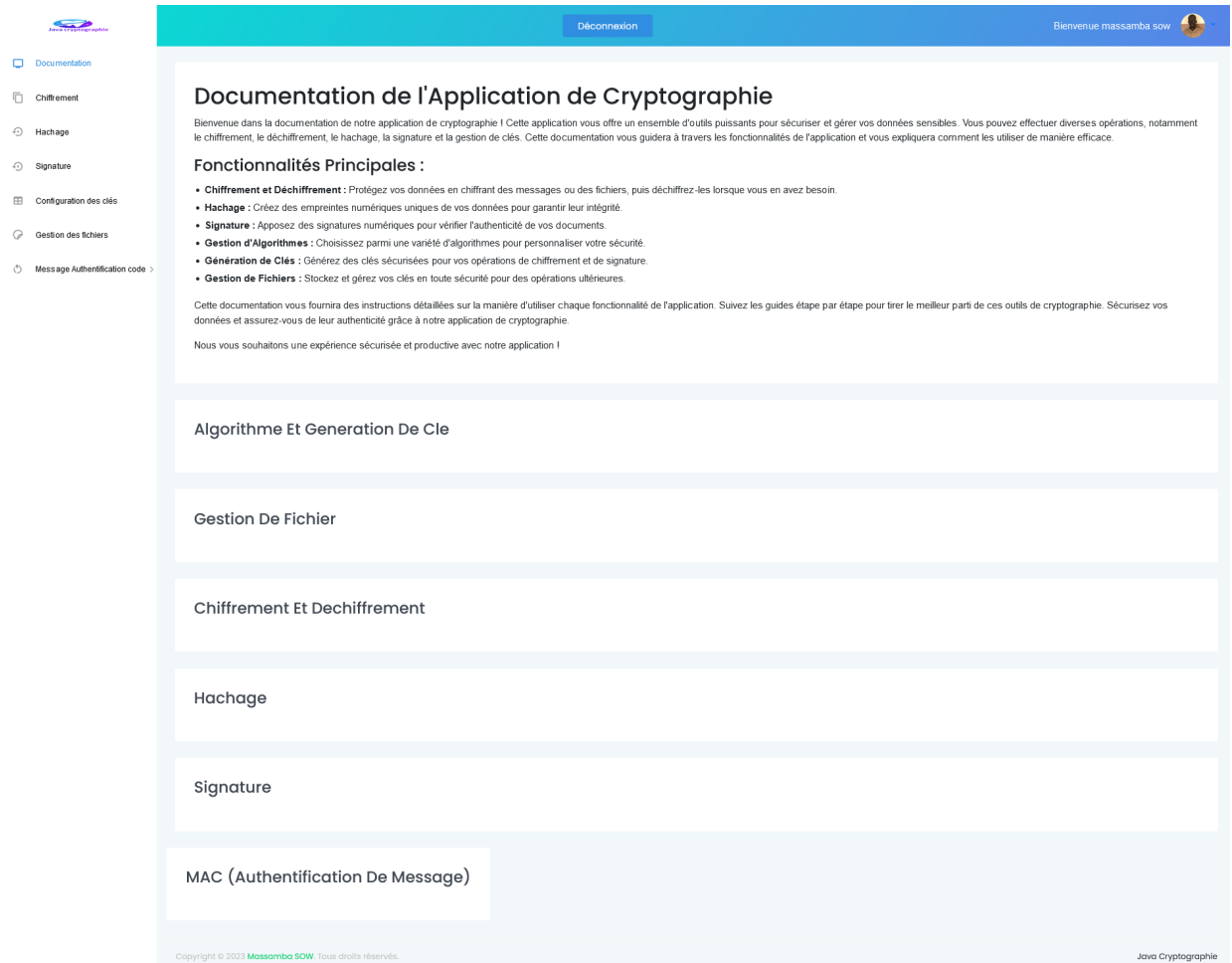
1. Choisissez le type d'algorithme que vous souhaitez utiliser parmi les options : symétrique, asymétrique, signature, clé partagée.
2. Choisissez un algorithme cryptographique parmi ceux disponibles.
3. Cliquez sur "Ajouter l'algorithme". L'algorithme sera ajouté à la liste des algorithmes disponibles pour l'utilisateur connecté.

Génération de Clé

1. Choisissez un algorithme dans la liste des algorithmes disponibles pour l'utilisateur connecté.
2. Choisissez la taille de la clé.
3. Ensuite, si vous cochez la case "Voulez-vous sauvegarder la clé":
 - Si oui, un champ d'entrée s'affichera pour que vous puissiez entrer le nom du fichier. Ce fichier sera sauvegardé dans la base de données et vous pourrez l'utiliser ultérieurement.
 - Si non, le fichier de clé sera téléchargé :
 - Si le type d'algorithme est symétrique, la clé générée sera un seul fichier avec comme nom "date_cle_secrete.sk"
 - Si le type d'algorithme est asymétrique ou signature, le fichier téléchargé sera un fichier ZIP contenant la clé publique et la clé privée avec comme nom "date_cle_publique_prive.zip".
4. Enfin, si vous cliquez sur "Générer", le fichier de clé sera téléchargé.

Gestion De Fichier

Chiffrement Et Dechiffrement



3. Gestion des algorithmes et génération de clés

Cette fonctionnalité permet à l'utilisateur d'ajouter des algorithmes qui seront utilisés dans la suite. Il faut noter que seuls les algorithmes ajoutés seront disponibles dans l'application. On distingue les algorithmes:

- Symétrique
- Asymétrique
- Hachage
- Signature numérique
- Message de Authentication code MAC

Pour créer un algorithme, il faut :

- ☐ Choisissez un type d'algorithme que vous souhaitez utiliser parmi les options précédemment énumérées.
- ☐ Choisissez un algorithme cryptographique parmi ceux disponibles.
- ☐ Cliquez sur Ajouter l'algorithme. L'algorithme sera ajouté à la liste des algorithmes disponibles pour l'utilisateur connecté.

Les algorithmes ajoutés seront enregistrés dans la base de données.

The screenshot shows a web application interface for Java Cryptographie. On the left is a sidebar menu with options: Documentation, Chiffrement, Hachage, Signature, Configuration des clés (highlighted), Gestion des fichiers, and Message Authentication code. The main content area has a blue header with a 'Déconnexion' button and a user greeting 'Bienvenue massamba sow' with a profile icon. There are two main panels:

- Ajouter Un Algorithme:** Contains a dropdown for 'Sélectionner le type d'algorithme:' with 'symétrique' selected, a dropdown for 'Nom algorithme' with 'AES' selected, a dropdown for 'Provider' with 'BC' selected, and an 'Ajouter l'algorithme' button.
- Generation De Cle:** Contains a dropdown for 'Sélectionner un algorithme:' with 'symétrique AES' selected, a dropdown for 'Taille' with '128' selected, a dropdown for 'Voulez-vous sauvegarder la clé ?' with 'Non' selected, and a 'Telecharger la cle' button.

At the bottom, there is a footer with 'Copyright © 2023 Massamba SOW. Tous droits réservés.' and 'Java Cryptographie'.

Pour générer une clé ou une paire de clés il faut :

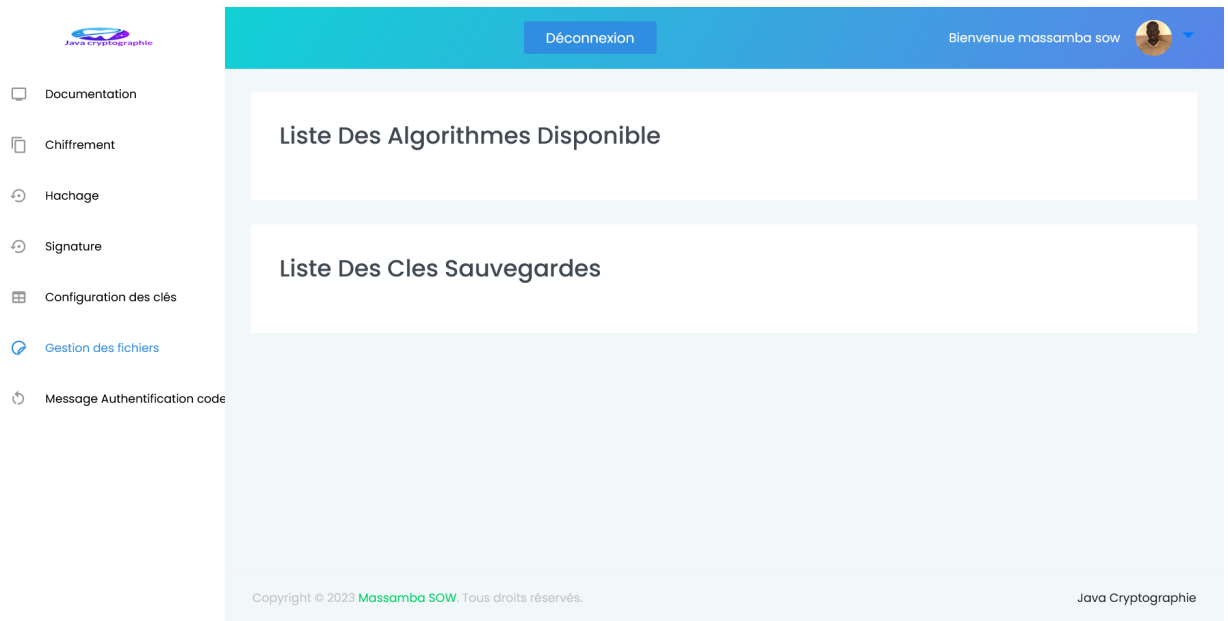
- ☐ Choisissez un algorithme dans la liste des algorithmes disponibles pour l'utilisateur connecté.
- ☐ Choisissez la taille de la clé.
- ☐ Ensuite, si vous cochez la case "Voulez-vous sauvegarder la clé":
 - Si oui, un champ d'entrée s'affiche pour que vous puissiez entrer le nom du fichier. Ce fichier sera sauvegardé dans la base de données et vous pourrez l'utiliser ultérieurement.
 - Si non, le fichier de clé sera téléchargé :
 - Si le type d'algorithme est symétrique, la clé générée sera un seul fichier avec comme nom "date_cle_secrete.sk".

- Si le type d'algorithme est asymétrique ou signature, le fichier téléchargé sera un fichier ZIP contenant la clé publique et la clé privée avec comme nom "date_cle_publique_prive.zip".

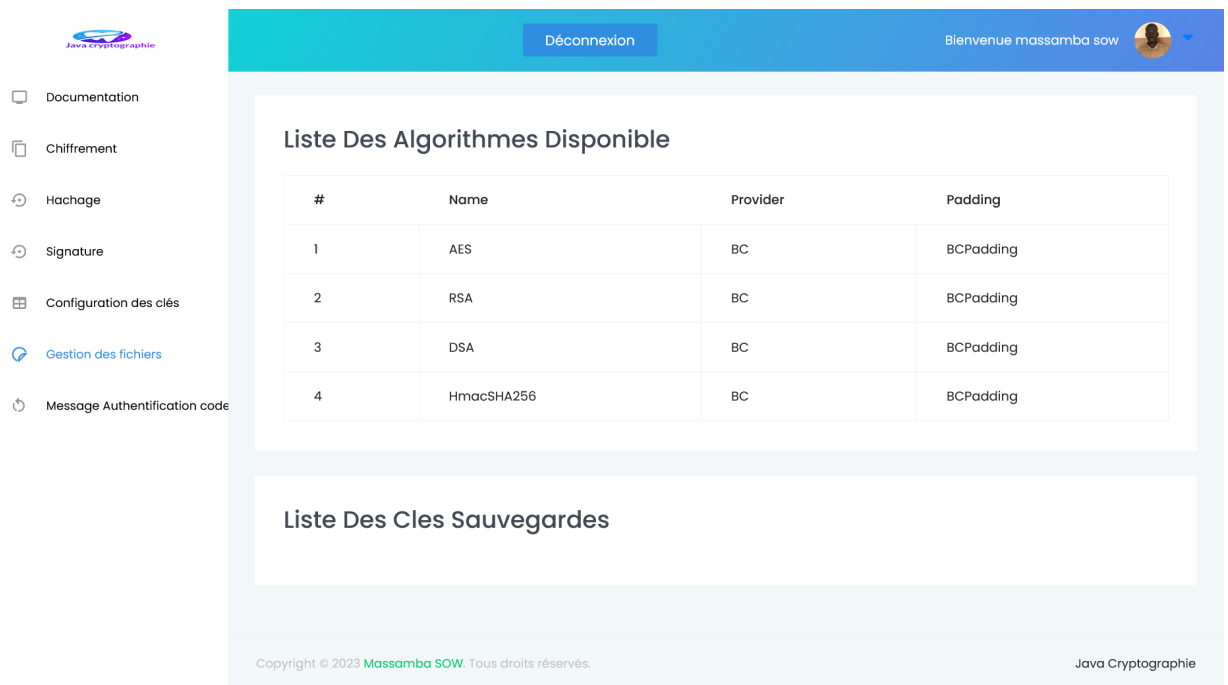
☐ Enfin, si vous cliquez sur "Générer", le fichier de clé sera téléchargé.

The screenshot displays the Java Cryptographie web application interface. On the left is a sidebar menu with the following items: Documentation, Chiffrement, Hachage, Signature, Configuration des clés (highlighted in blue), Gestion des fichiers, and Message Authentication code. The main content area is divided into two panels. The left panel, titled 'Ajouter Un Algorithme', contains a dropdown menu for 'Sélectionner le type d'algorithme:' with 'symetrique' selected, a text input for 'Nom algorithme' containing 'AES', a dropdown for 'Provider' with 'BC' selected, and a blue button labeled 'Ajouter l'algorithme'. The right panel, titled 'Generation De Cle', contains a dropdown for 'Sélectionner un algorithme:' with 'symetrique AES' selected, a dropdown for 'Taille' with '128' selected, a dropdown for 'Voulez-vous sauvegarder la clé ?' with 'Oui' selected, a text input for 'Nom du fichier :' containing 'cles', and a blue button labeled 'Enregistrer la cle'. The top of the interface has a blue header with a 'Déconnexion' button and a user profile section showing 'Bienvenue massamba sow' and a user icon. The footer contains the copyright notice 'Copyright © 2023 Massamba SOW. Tous droits réservés.' and the text 'Java Cryptographie'.

4. Gestion des clés



- La liste des algorithmes précédemment ajoutés sera affichés ici.L'utilisateur peut les visualiser.



- Les clés enregistrés par l'utilisateur sont affichés avec les informations suivantes :
 - **ID**

- **Type d'Algorithme**
- **Nom de l'Algorithme**
- **Date de création**
- **Action**

Dans la colonne "**Action**", l'utilisateur peut télécharger la clé pour l'utiliser.

Il peut aussi supprimer la clé, dans ce cas la clé ne sera plus disponible.

The screenshot shows the Java Cryptographie application interface. On the left is a sidebar with navigation links: Documentation, Chiffrement, Hachage, Signature, Configuration des clés, Gestion des fichiers (highlighted), and Message Authentication code. The main content area has a top header with a 'Déconnexion' button and a user greeting 'Bienvenue massamba sow'. Below this, there are two sections: 'Liste Des Algorithmes Disponible' and 'Liste Des Cles Sauvegardes'. The 'Liste Des Cles Sauvegardes' section contains a table with the following data:

nom algorithme	type	taille	Date de sauvegarde	Actions
AES	symetrique	128	2023-10-26	Telecharger Supprimer

At the bottom of the page, there is a copyright notice: 'Copyright © 2023 Massamba SOW. Tous droits réservés.' and the text 'Java Cryptographie'.

5. Chiffrement et Déchiffrement

L'application de chiffrement offre les fonctionnalités suivantes :

- ☐ Chiffrer des messages ou des fichiers
- ☐ Déchiffrer des messages ou des fichiers

A. Pour le chiffrement :

- a. Sélectionnez le type d'algorithme de chiffrement. Par exemple, AES.
- b. Entrez une clé de chiffrement symétrique (la clé doit être obligatoirement une clé symétrique, sinon une erreur se produira et vous serez redirigé vers une autre page).
- c. Saisissez les données à chiffrer. Vous pouvez soit entrer un message, soit importer un fichier.
- d. Enfin, cliquez sur "Chiffrer" pour obtenir le résultat chiffré.

B. Pour le déchiffrement :

- a. Sélectionnez le type d'algorithme de chiffrement. Par exemple, AES.
- b. Entrez une clé symétrique (la clé doit être obligatoirement une clé symétrique, sinon une erreur se produira et vous serez redirigé vers une autre page).
- c. Saisissez les données à chiffrer.Importer un fichier : la clé symétrique.
- d. Enfin, cliquez sur "Déchiffrer" pour obtenir le texte déchiffré.

NB: Assurez-vous de conserver vos clés de chiffrement en sécurité.

The screenshot displays the Java Cryptographie application interface. On the left is a sidebar with navigation links: Documentation, Chiffrement (highlighted), Hachage, Signature, Configuration des clés, Gestion des fichiers, and Message Authentification code. The main area is split into two panels: 'Chiffrement' (Encryption) and 'Déchiffrement' (Decryption). Both panels have a dropdown menu for 'Sélectionner un algorithme:' set to 'symétrique AES' and an 'Importer une clé' button. The 'Chiffrement' panel shows 'Clé de chiffrement sélectionnée : 2023-10-26_cle_secret.key', a dropdown for 'Choisir entre un message ou un fichier:' set to 'Fichier', a 'Choisir un fichier' button, and 'fichier selectionne : Cours_Crypto-Java_JCA-JCE.pdf' with a 'Chiffrer' button. The 'Déchiffrement' panel shows the same key, dropdown, and button, with 'fichier selectionne : fichier-crypte(7).txt' and a 'Dechiffrer' button. The top bar includes a 'Déconnexion' button and a user profile 'Bienvenue massamba sow'. The footer contains copyright information: 'Copyright © 2023 Massamba SOW. Tous droits réservés.' and 'Java Cryptographie'.


6. Hachage et Vérification de hachage


La fonction de hachage est utilisée pour créer une empreinte numérique unique d'une donnée, que ce soit un message ou un fichier. Vous pouvez également vérifier l'authenticité d'une donnée en comparant son empreinte avec une empreinte préalablement calculée.

A. Création d'un Hachage

- i. Sélectionnez l'algorithme de hachage que vous souhaitez utiliser, par exemple, SHA-256.
- ii. Entrez le texte ou le fichier que vous souhaitez hacher.
- iii. Cliquez sur "Hacher" pour obtenir l'empreinte numérique.

NB : Assurez-vous de noter l'algorithme de hachage utilisé et l'empreinte générée, car vous en aurez besoin pour vérifier le hachage plus tard.

 Documentation
Chiffrement
Hachage
Signature
Configuration des clés
Gestion des fichiers
Message Authentication code

[Déconnexion](#)Bienvenue massamba sow

Hachage De Message

Sélectionner un algorithme de hachage

Hachage :SHA-256

Taille

256

Choisir entre un message ou un fichier :

Message

Message :

massamba sow

Calculer l'empreinte

Verification De Hache

Sélectionner un algorithme de hachage

Choisir un algorithme

Choisir entre un message ou un fichier :

Message

Message :

Empreinte

Vérifier

Resultat

6fd9l8c7ab2a9589229dc68af547b38cab0ecc2c56d4db01b334dl64862c303f

Copyright © 2023 Massamba SOW. Tous droits réservés.

Java Cryptograph

B. Vérification du Hachage

Sélectionnez le même algorithme de hachage utilisé précédemment, par exemple, SHA-256.

1. Entrez le texte ou le fichier que vous souhaitez vérifier.
2. Entrez l'empreinte numérique précédemment calculée.
3. Cliquez sur "Vérifier Hachage".

NB : L'application compare l'empreinte numérique de la donnée avec l'empreinte précédemment calculée. Si elles correspondent, la donnée est authentique.

- Documentation
- Chiffrement
- Hachage**
- Signature
- Configuration des clés
- Gestion des fichiers
- Message Authentication code

Déconnexion

Bienvenue massamba sow

Hachage De Message

Sélectionner un algorithme de hachage

Hachage :SHA-256

Taille

256

Choisir entre un message ou un fichier :

Fichier

Choisir un fichier

Calculer l'empreinte

Verification De Hache

Sélectionner un algorithme de hachage

Hachage :SHA-256

Choisir entre un message ou un fichier :

Fichier

Choisir un fichier

fichier selectionne :
Cours_Crypto-Java_JCA-JCE.pdf

Empreinte

1eff0e8f30352d420413b7d6bc428a7860dd5e366e4c46ee37eb962c1e98ddea

Verifier

Resultat



Fichier : Cours_Crypto-Java_JCA-JCE.pdf

Hash : 1eff0e8f30352d420413b7d6bc428a7860dd5e366e4c46ee37eb962c1e98ddea

Verification réussi Reinitialiser

Copyright © 2023 Massamba SOW. Tous droits réservés.

Java Cryptographie

DéconnexionBienvenue massamba sow

Documentation

Chiffrement

Hachage

Signature

Configuration des clés

Gestion des fichiers

Message Authentication code

Hachage De Message

Sélectionner un algorithme de hachage

Hachage :SHA-256

Taille

256

Choisir entre un message ou un fichier :

Fichier

Choisir un fichier

Calculer l'empreinte

Verification De Hache

Sélectionner un algorithme de hachage

Hachage :SHA-256

Choisir entre un message ou un fichier :

Fichier

Choisir un fichier

fichier selectionne : Cours_Crypto-Java_JCA-JCE.pdf

Empreinte

1etf0e8f30352d420413b7d6bc428a7860dd5e366e4c46ee37eb962c1e98ddea

Verifier

Resultat

Fichier : Cours_Crypto-Java_JCA-JCE.pdf

Hash : 1etf0e8f30352d420413b7d6bc428a7860dd5e366e4c46ee37eb962c1e98ddea

Verification echoue Reinitialiser

Copyright © 2023 Massamba SOW. Tous droits réservés. Java Cryptographie

7. Signature et Vérification de signature

La signature numérique permet de vérifier l'authenticité d'un document en utilisant un algorithme asymétrique. Vous pouvez créer une signature numérique pour un message ou un fichier, puis vérifier la signature pour vous assurer qu'elle n'a pas été altérée.

a. Création d'une Signature

- Sélectionnez l'algorithme asymétrique que vous souhaitez utiliser, par exemple, RSA.
- Sélectionnez l'algorithme de signature correspondant, par exemple, RSA-SHA256.
- Entrez votre clé privée correspondant à l'algorithme asymétrique choisi.
- Entrez le texte ou le fichier que vous souhaitez signer.

14

- v. Cliquez sur "Signer" pour créer la signature numérique.

La signature sera générée pour le message ou le fichier, assurez-vous de conserver votre clé privée en sécurité.


The screenshot displays the Java Cryptographie web application interface. On the left is a sidebar menu with options: Documentation, Chiffrement, Hachage, Signature (highlighted), Configuration des clés, Gestion des fichiers, and Message Authentication code. The main content area is divided into two panels: 'Signature De Message' and 'Verification De Signature'. The 'Signature De Message' panel includes a dropdown for 'Sélectionner un algorithme de asymetrique' (set to 'Signature : DSA'), a dropdown for 'Algorithme de signature' (set to 'SHA256withDSA'), a button 'Entrer votre clé privée' with a 'cle.priv' input field, a dropdown for 'Choisir entre un message ou un fichier' (set to 'Fichier'), a 'Choisir un fichier' button, and a display of the selected file 'Cours_Crypto-Java_JCA-JCE.pdf' with a 'Calculer l'empreinte' button. The 'Verification De Signature' panel includes a dropdown for 'Sélectionner un algorithme de asymetrique' (set to 'Choisir un algorithme'), a dropdown for 'Algorithme de signature', a button 'Entrer votre clé publique', a dropdown for 'Choisir entre un message ou un fichier' (set to 'Message'), a 'Message :' input field, an 'Empreinte' input field, and a 'Verifier' button. At the bottom, a 'Resultat' section shows a long hexadecimal string. The footer contains copyright information for 2023 Massamba SOW and the Java Cryptographie logo.

b. Vérification de la Signature

- i. Sélectionnez le même algorithme asymétrique que celui utilisé pour la signature, par exemple, RSA.
- ii. Sélectionnez le même algorithme de signature correspondant, par exemple, RSA-SHA256.
- iii. Entrez votre clé publique correspondant à l'algorithme asymétrique choisi.
- iv. Entrez le texte ou le fichier que vous souhaitez vérifier.

- v. Entrez la signature précédemment calculée.
- vi. Cliquez sur "Vérifier" pour vérifier la signature numérique.

L'application compare la signature numérique de la donnée avec la signature précédemment calculée. Si elles correspondent, la donnée est authentique et n'a pas été altérée.



Documentation

Chiffrement

Hachage


Signature

Configuration des clés

Gestion des fichiers

Message Authentication code

Déconnexion

Bienvenue massamba sow 

Signature De Message

Sélectionner un algorithme de asymetrique

Signature : DSA

Algorithme de signature

SHA256withDSA

Entrer votre clé privée

cle.priv

Choisir entre un message ou un fichier :

Fichier

Choisir un fichier

Calculer l'empreinte

Verification De Signature

Sélectionner un algorithme de asymetrique

Signature : DSA

Algorithme de signature

SHA256withDSA

Entrer votre clé publique

cle.pub

Choisir entre un message ou un fichier :

Fichier

Choisir un fichier

fichier selectionne :
Cours_Crypto-Java_JCA-JCE.pdf

Empreinte

302c02143e9b72c530bcf7ff0e011daa5a13f92620d0119b0214058444e2d2cd24f7f2e11798a642254d48ee066b

Vérifier

Resultat

Fichier : Cours_Crypto-Java_JCA-JCE.pdf


Signature : 302c02143e9b72c530bcf7ff0e011daa5a13f92620d0119b0214058444e2d2cd24f7f2e11798a642254d48ee066b

Verification réussi

Reinitialiser


Copyright © 2023 Massamba SOW. Tous droits réservés.

Java Cryptographie



- Documentation
- Chiffrement
- Hachage
- Signature**
- Configuration des clés
- Gestion des fichiers
- Message Authentication code

Déconnexion

Bienvenue massamba sow 

Signature De Message

Sélectionner un algorithme de asymetrique

Signature : DSA

Algorithme de signature

SHA256withDSA

Entrer votre clé privée cle.priv

Choisir entre un message ou un fichier :

Fichier

Choisir un fichier

Calculer l'empreinte

Verification De Signature

Sélectionner un algorithme de asymetrique

Signature : DSA

Algorithme de signature

SHA256withDSA

Entrer votre clé publique cle.pub

Choisir entre un message ou un fichier :

Fichier

Choisir un fichier

fichier selectionne : Cours_Crypto-Java_JCA-JCE.pdf

Empreinte

302c02143e9b72c530bcf7ff0e011daa5a13f92620d0119b0214058444e2d2cd24f7f2e11798a642254d48ee066y

Verifier

Resultat

Fichier : Cours_Crypto-Java_JCA-JCE.pdf

Signature : 302c02143e9b72c530bcf7ff0e011daa5a13f92620d0119b0214058444e2d2cd24f7f2e11798a642254d48ee066y

Verification echoue Reinitialiser

Copyright © 2023 Massamba SOW. Tous droits réservés.

Java Cryptographie

8. Création de Message Authentication Code (MAC)

Un MAC (Message Authentication Code) est une valeur de hachage cryptographique générée à partir d'un message et d'une clé secrète. Il est utilisé pour vérifier l'intégrité et l'authenticité du message, c'est-à-dire pour s'assurer qu'il n'a pas été modifié en transit et qu'il provient bien de la source prévue.

- Authentification : Le MAC garantit que le message n'a pas été altéré pendant la transmission, ce qui aide à prévenir les attaques de type "man-in-the-middle".
- Intégrité : Il assure que le message n'a pas été modifié par des tiers non autorisés.

-
- Confidentialité : Le MAC ne chiffre pas le message, mais il utilise la clé secrète pour vérifier l'authenticité du message.
 - Clé secrète : Pour générer un MAC, une clé secrète est utilisée, ce qui rend la vérification du MAC impossible sans cette clé.


L'application de génération de MAC offre un moyen simple de créer un MAC en fonction de vos besoins. Suivez les étapes ci-dessous pour utiliser cette fonctionnalité.

- Générer un MAC pour l'authentification de message ou de fichier.

Pour générer un MAC :


1. Sélectionnez l'algorithme de MAC que vous souhaitez utiliser. Par exemple, HMAC-SHA256.
2. Choisissez entre une clé secrète ou un mot de passe pour l'authentification. La clé secrète sera générée en fonction de l'option choisie.
3. Indiquez si vous souhaitez authentifier un message ou un fichier.
4. Saisissez le message ou importez le fichier que vous souhaitez authentifier.
5. Cliquez sur "Générer MAC" pour obtenir le résultat du MAC.

Remarque : Assurez-vous de conserver votre clé secrète ou mot de passe en toute sécurité, car ils sont essentiels pour la génération du MAC.



Documentation
Chiffrement
Hachage
Signature
Configuration des clés
Gestion des fichiers
Message Authentication code

Déconnexion

Bienvenue massamba sow 

Ceration De Message Authentication Code (MAC)

Sélectionner un algorithme:

MAC: HmacSHA256

Mot de passe PBE:

•••••

Choisir entre message et fichiers:

Message

Message:

massamba


Générer le MAC

Resultat

f72539135561b796265e49fcb648309d24172e541bb1c641e152b17ef8064302


Copyright © 2023 [Massamba SOW](#). Tous droits réservés.

Java Cryptographie



Documentation
Chiffrement
Hachage
Signature
Configuration des clés
Gestion des fichiers
Message Authentication code

Déconnexion

Bienvenue massamba sow 

Ceration De Message Authentication Code (MAC)

Sélectionner un algorithme:

MAC: HmacSHA256

Mot de passe PBE:

••••••••

Choisir entre message et fichiers:

Fichiers

Parcourir... Cours_Crypto-Java_JCA-JCE.pdf

Générer le MAC

Resultat

3367cff39e156c9d07a9507211a6a6c47cf89d57a7c88857a00845583704df4c

Copyright © 2023 [Massamba SOW](#). Tous droits réservés.

Java Cryptographie

9. Conclusion

L'Application de Cryptographie offre un ensemble complet d'outils de sécurité pour protéger vos données sensibles. Ce rapport présente les fonctionnalités clés de l'application et fournit des instructions sur la manière de les utiliser. Assurez-vous de suivre les guides étape par étape pour garantir la sécurité et l'authenticité de vos données. Nous vous souhaitons une expérience sécurisée et productive avec notre application !