Lucrarea de laborator nr. 6

Criptografie aplicată și integritatea datelor

Scop

Scopul lucrării este aplicarea practică a conceptelor fundamentale de criptografie prin utilizarea algoritmilor de criptare simetrică și asimetrică, a semnăturilor digitale și a funcțiilor hash pentru asigurarea confidențialității, autenticității și integrității datelor.

Cerință generală

Implementați și demonstrați utilizarea **criptării simetrice (AES)**, **criptării asimetrice (RSA)**, **semnăturii digitale** și **funcțiilor hash (SHA-256)** pentru protecția datelor. Analizați diferențele de performanță și utilizare dintre metodele aplicate.

Cerințe obligatorii

1. Pregătirea mediului de lucru

Indicați:

- sistemul de operare utilizat;
- instrumentele sau bibliotecile utilizate pentru criptografie;
- tipul de fișiere sau date utilizate pentru testare.

2. Criptare simetrică (AES)

Implementați criptarea simetrică utilizând algoritmul **AES**, indicând:

- modul de utilizare (criptare/decriptare);
- dimensiunea cheii utilizate;
- demonstrarea accesului la date înainte și după criptare.

3. Criptare asimetrică (RSA)

Implementați criptarea asimetrică utilizând **RSA**, indicând:

- procesul de generare a cheilor;
- criptarea și decriptarea unui mesaj sau fișier;
- rolul cheilor publice și private.

4. Semnătura digitală

Implementați un mecanism de **semnătură digitală**, indicând:

- datele semnate;
- procesul de semnare;
- procesul de verificare a semnăturii.

5. Verificarea integrității datelor (Hashing)

Utilizați o funcție hash criptografică (**SHA-256**) pentru:

- calcularea valorii hash a unui fișier;
- modificarea fișierului;
- verificarea schimbării valorii hash.

6. Analiza comparativă

Realizați o analiză comparativă care să includă:

- diferențele dintre criptarea simetrică și asimetrică;
- avantajele și limitările fiecărei metode;
- impactul asupra performanței.

Лабораторная работа №6

Прикладная криптография и целостность данных

Цель работы

Целью данной лабораторной работы является практическое применение фундаментальных концепций криптографии с использованием алгоритмов симметричного и асимметричного шифрования, цифровых подписей и хеш-функций для обеспечения конфиденциальности, подлинности и целостности данных.

Общее требование

Реализуйте и продемонстрируйте использование симметричного шифрования (AES), асимметричного шифрования (RSA), цифровой подписи и криптографических хеш-функций (SHA-256) для защиты данных. Проанализируйте различия в производительности и областях применения используемых методов.

Обязательные требования

1. Подготовка рабочей среды

Укажите:

- используемую операционную систему;
- инструменты или библиотеки, применяемые для криптографии;
- тип файлов или данных, используемых для тестирования.

2. Симметричное шифрование (AES)

Реализуйте симметричное шифрование с использованием алгоритма **AES**, указав:

- режим использования (шифрование/дешифрование);
- размер используемого ключа;
- демонстрацию доступа к данным до и после шифрования.

3. Асимметричное шифрование (RSA)

Реализуйте асимметричное шифрование с использованием **RSA**, указав:

- процесс генерации ключей;
- шифрование и дешифрование сообщения или файла;
- роль открытого и закрытого ключей.

4. Цифровая подпись

Реализуйте механизм **цифровой подписи**, указав:

- подписываемые данные;
- процесс создания подписи;
- процесс проверки подписи.

5. Проверка целостности данных (Hashing)

Используйте криптографическую хеш-функцию **SHA-256** для:

- вычисления хеш-значения файла;
- изменения файла;
- проверки изменения хеш-значения.

6. Сравнительный анализ

Выполните сравнительный анализ, включающий:

- различия между симметричным и асимметричным шифрованием;
- преимущества и ограничения каждого метода;
- влияние на производительность.