Алгоритм DES (Data Encryption Standard)  
  
Алгоритм DES (Data Encryption Standard) є одним з найбільш відомих та широко використовуваних симетричних алгоритмів шифрування. Він був розроблений у 1970-х роках та використовувався для захисту конфіденційності даних у різних сферах, включаючи електронну комунікацію та фінансові транзакції.

Переваги DES:

Висока швидкодія: DES був проектований для шифрування на рівні апаратури, що забезпечує його високу продуктивність. Він може шифрувати та розшифровувати великі обсяги даних швидко.

Широке застосування: DES був широко використовуваний в багатьох сферах, і його підтримують багато програм та пристроїв.

Криптографічна стійкість: DES надавав високий рівень безпеки на момент свого виникнення, тобто в 1970-х роках. Він забезпечував достатню захист від багатьох атак того часу.

Недоліки DES:

Короткий ключ: DES використовує 56-бітний ключ, що становить вразливість у сучасних обчислювальних умовах. Швидкість розвитку обчислювальної потужності та криптоаналітичних методів зробили його вразливим до підбору ключа методом перебору.

Можливість атаки на структуру: DES має певні структурні вразливості, що дозволяють побудувати ефективні атаки, такі як "Meet-in-the-Middle" атака.

Вік стандарту: DES був стандартизований у 1977 році, і з того часу криптографічні методи та атаки значно продовжили свій розвиток. Його використання в сучасних системах не рекомендується через його обмежену стійкість до поточних криптоаналітичних атак.

У зв'язку з недоліками DES, у 2001 році його було витіснено більш безпечним стандартом AES (Advanced Encryption Standard), який використовує ключ довжиною 128 біт або більше і забезпечує вищий рівень стійкості.  
  
  
  
  
  
  
SHA-1 (Secure Hash Algorithm 1) є криптографічною хеш-функцією, що використовується для перетворення даних відмінних розмірів в фіксований хеш-код фіксованої довжини 160 бітів (20 байтів). Вона була розроблена Штатним інститутом стандартів і технологій США (NIST) і вперше опублікована в 1995 році.

Переваги SHA-1:

Простота реалізації: SHA-1 є досить простою в реалізації і використанні, що робить її доступною для багатьох платформ та мов програмування.

Швидкість: SHA-1 є відносно швидкою хеш-функцією, і обчислення хеш-коду можуть проводитись досить ефективно.

Використовується в старіших системах: SHA-1 досі використовується в деяких старіших системах і протоколах, які ще не були оновлені до більш безпечних алгоритмів хешування.

Недоліки SHA-1:

Вразливість до зламу: SHA-1 не є безпечним для криптографічних застосувань і піддається атакам, таким як зіткнення. У 2005 році була опублікована атака, яка дозволила знайти зіткнення хеш-кодів швидше, ніж було очікувано. У 2017 році NIST рекомендував припинити використання SHA-1 для криптографічних застосувань.

Відсутність аутентичності: SHA-1 не забезпечує аутентичності даних. Це означає, що неможливо перевірити, чи були дані змінені після обчислення хеш-коду.

Застаріла технологія: З часом SHA-1 стала застарілою технологією, і більш безпечні альтернативи, такі як SHA-256, SHA-384 та SHA-512, були розроблені для забезпечення кращої безпеки.