КУРСОВА РОБОТА

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ І НАДІЙНОСТІ АЛГОРИТМІВ ШИФРУВАННЯ

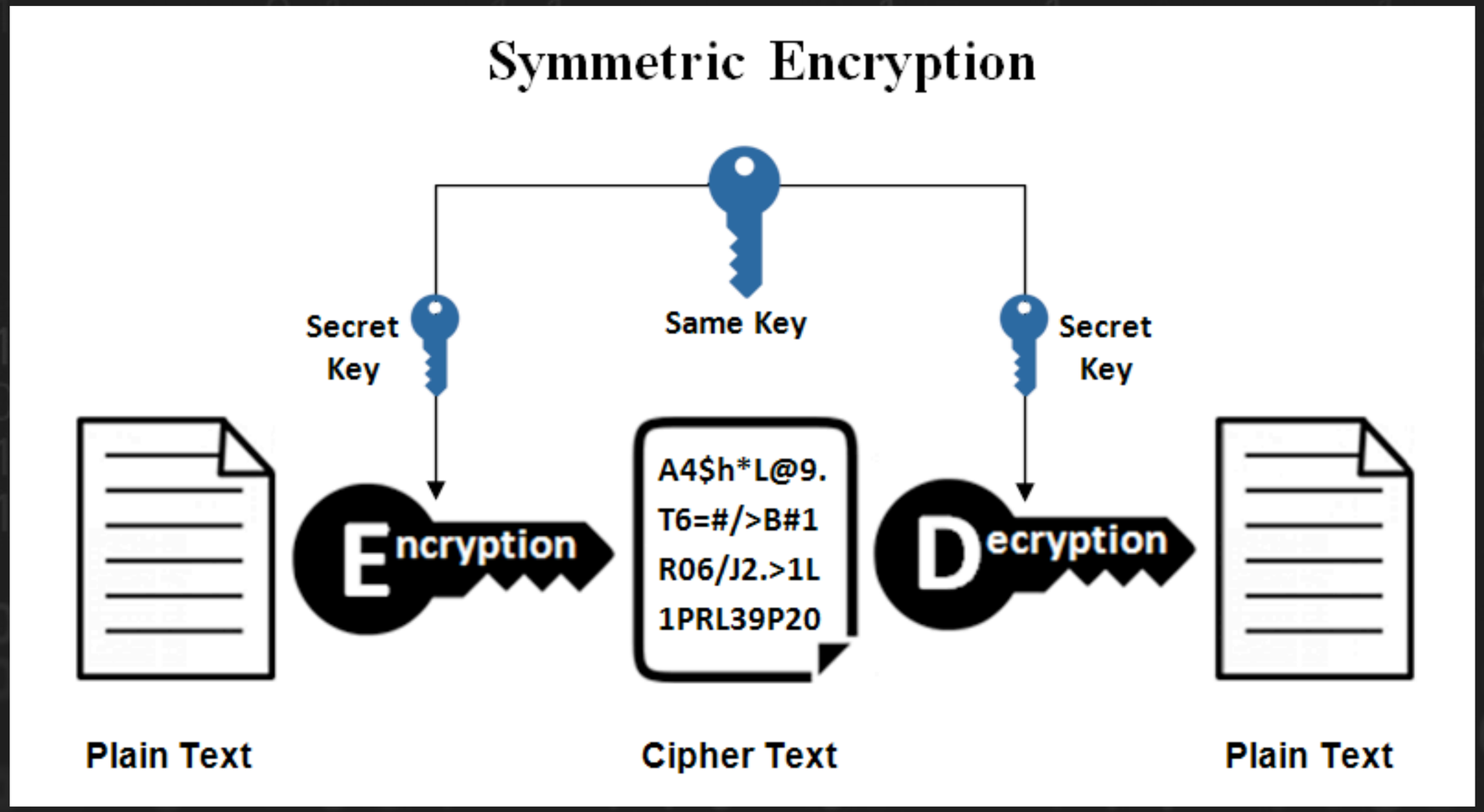
АКТУАЛЬНІСТЬ РОБОТИ

ШИФРУВАННЯ – ЦЕ …

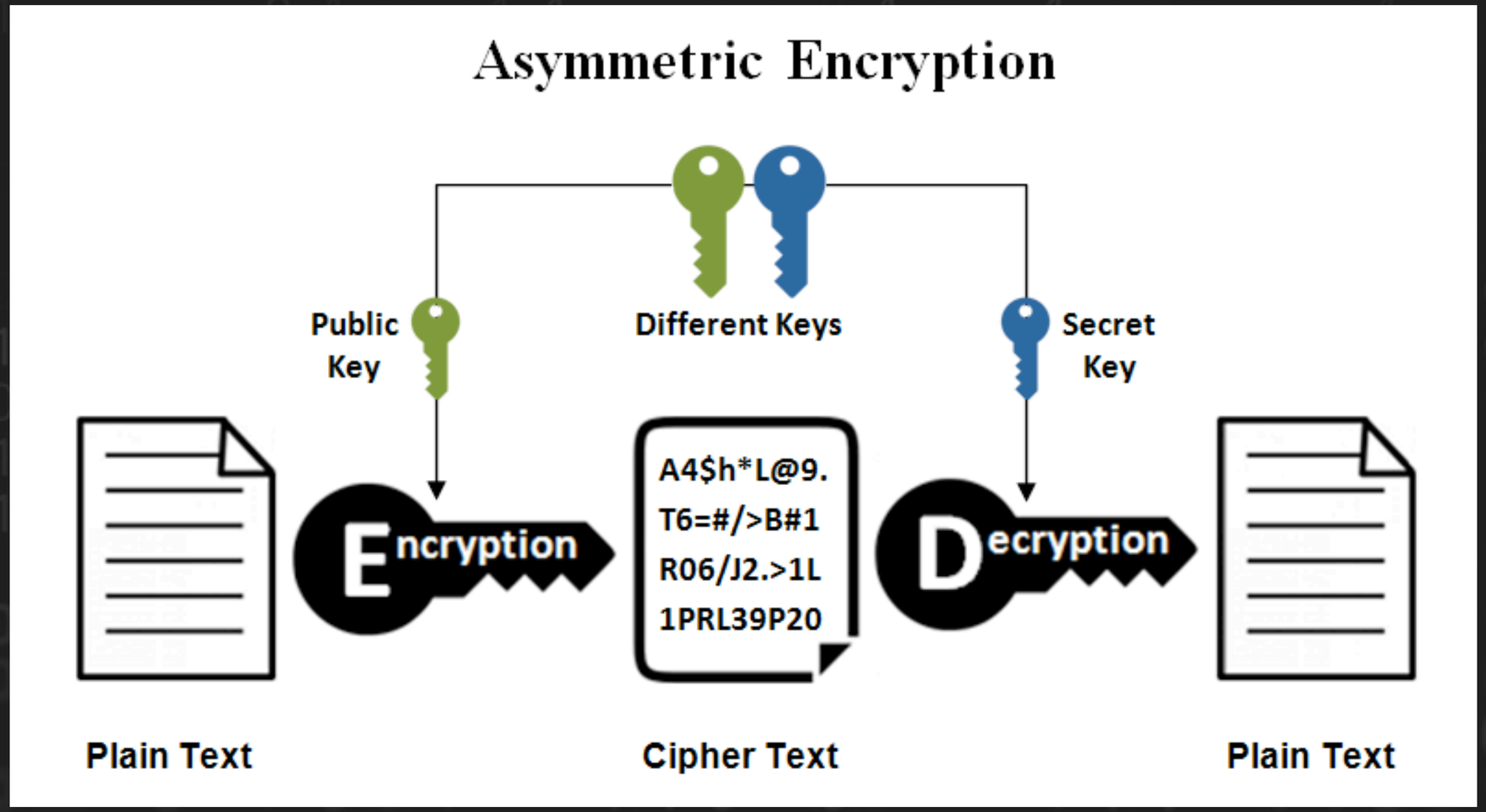
ЕТАПИ РОЗВИТКУ ШИФРУВАННЯ

- Стародавні часи
- Середньовіччя і Ренесанс
- Ера машинного шифрування
- Ера комп’ютерного шифрування
- Сучасна ера

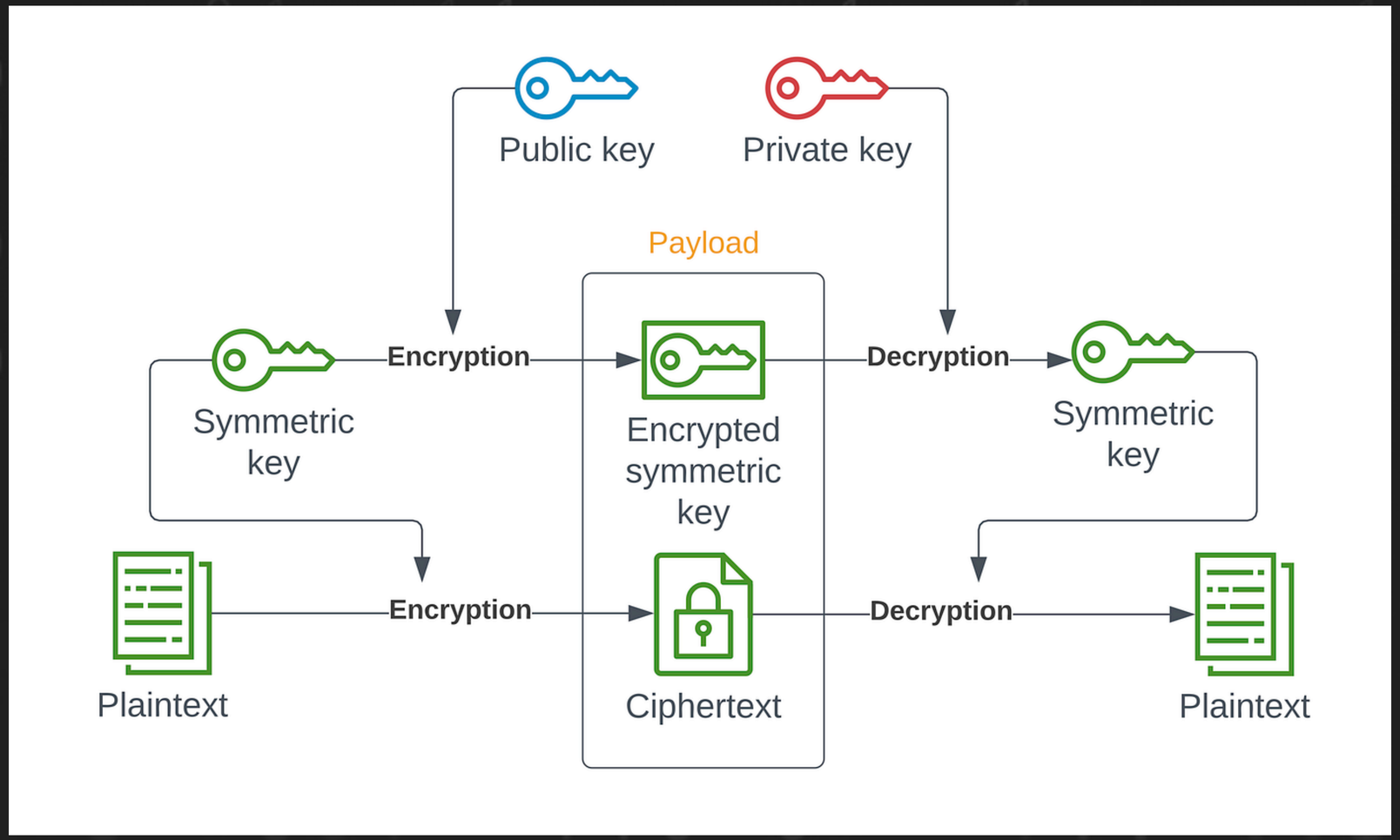
СИМЕТРИЧНЕ ШИФРУВАННЯ



АСИМЕТРИЧНЕ ШИФРУВАННЯ



ГІБРИДНЕ ШИФРУВАННЯ

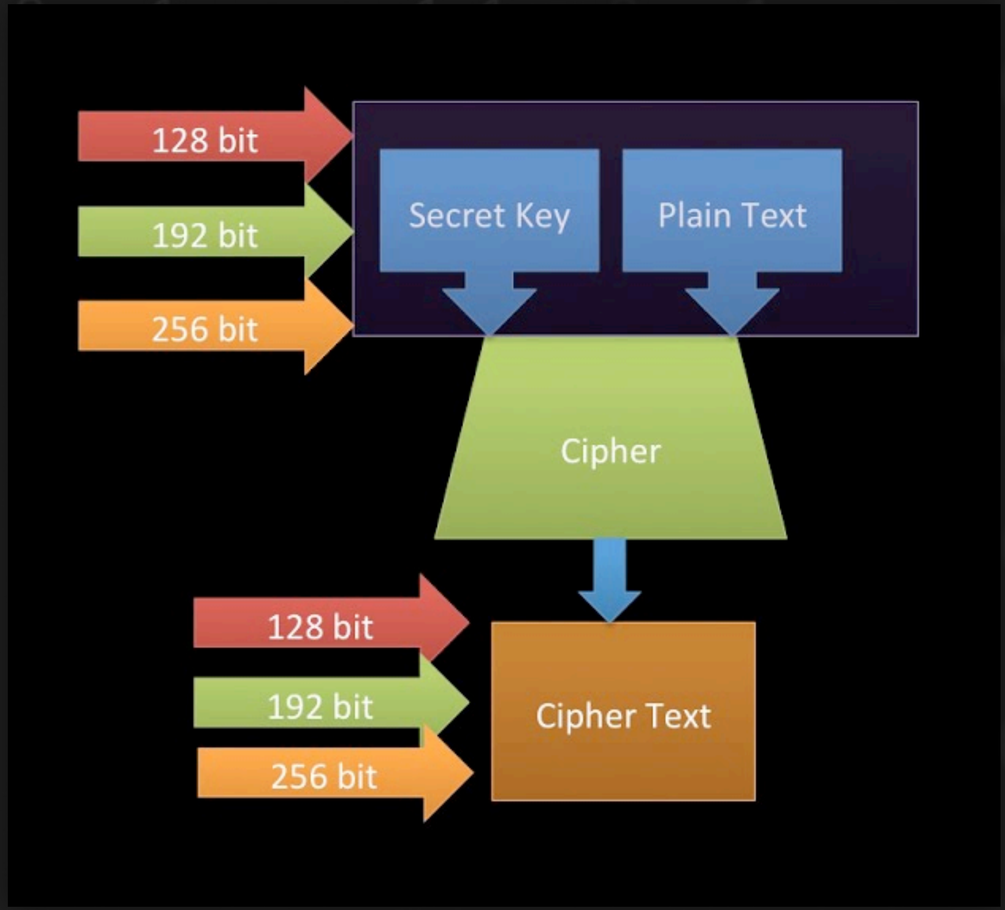


КЛЮЧОВІ ФАКТОРИ ЕФЕКТИВНОСТІ ТА НАДІЙНОСТІ АЛГОРИТМІВ ШИФРУВАННЯ

- Складність атак
- Довжина ключа
- Швидкодія
- Ресурсоємність
- Ключове управління
- Математична стійкість
- Безпека
- Розмір ключа
- Використання пам'яті

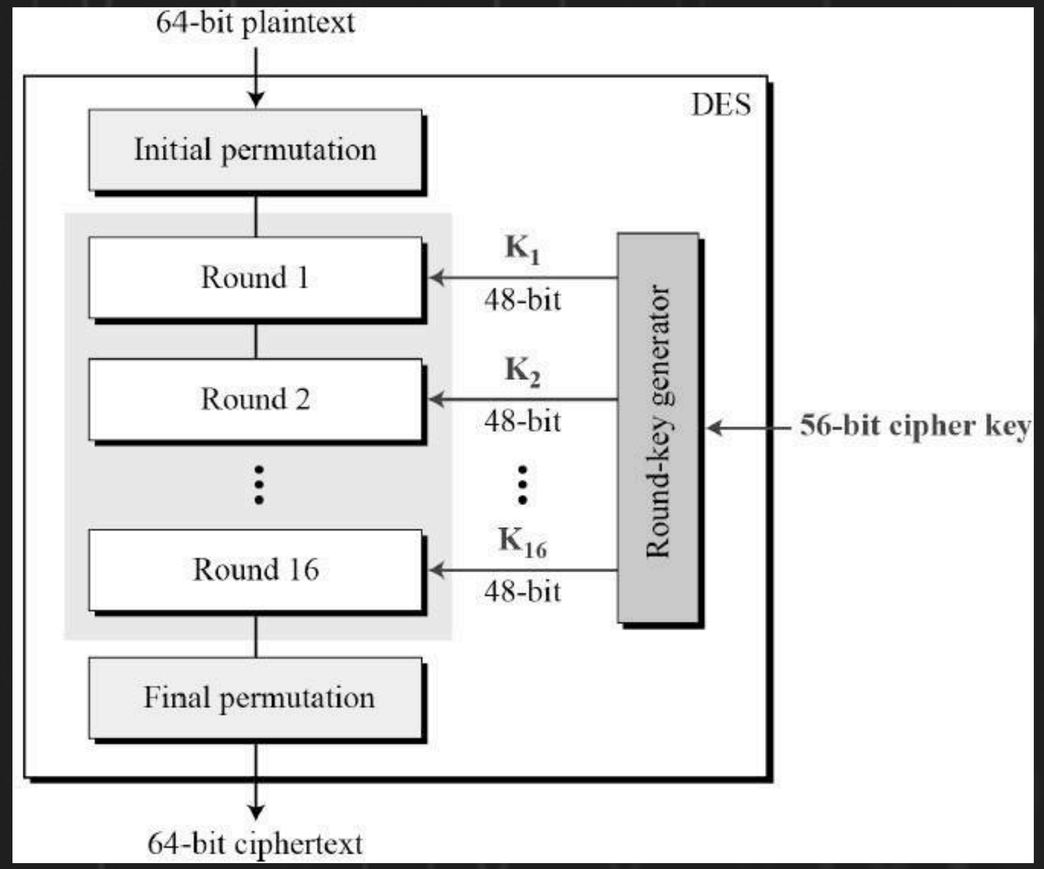
АЛГОРИТМ AES

- Симетричний алгоритм блочного шифрування
- Прийнятий як стандарт шифрування у США
- Три різновиди блок-шифрів: AES-128, AES-192 та AES-256
- Використовує той самий ключ для кодування та декодування



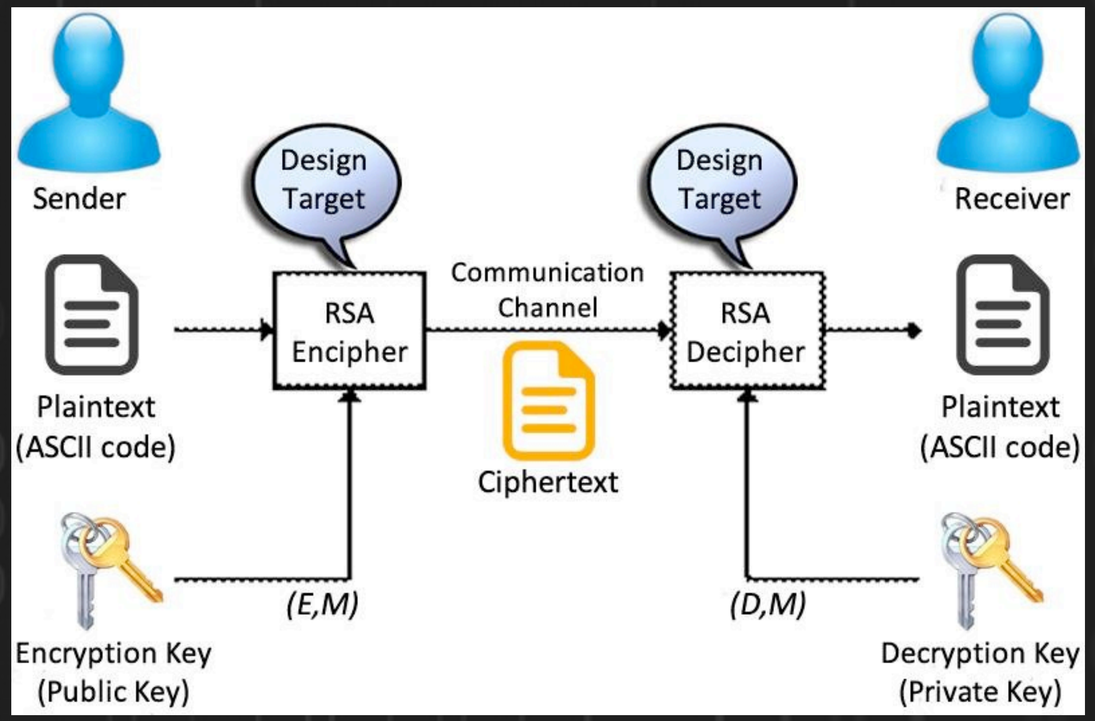
АЛГОРИТМ DES

- Симетричний алгоритм блочного шифрування
- Стандартизований в 1970-х роках Федеральним інститутом стандартів США (NIST)
- Включає 16 раундів або циклів трансформацій
- Дав поштовх сучасним уявленням про криптоаналіз



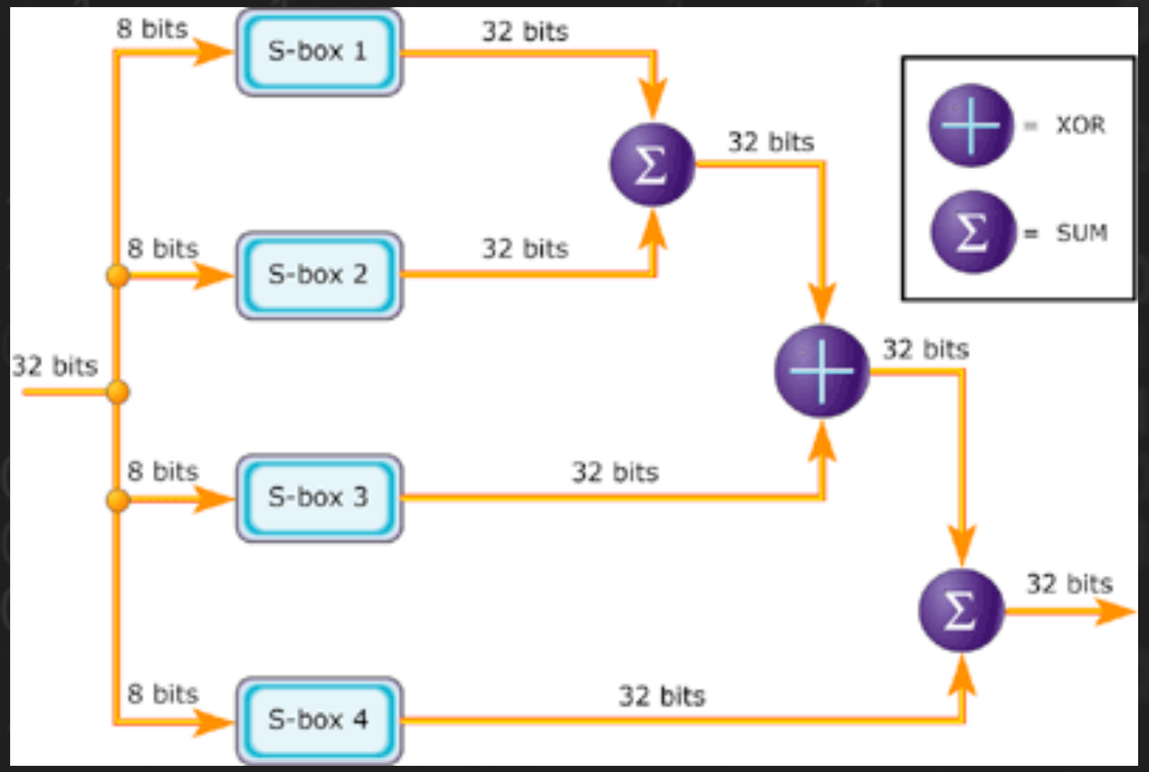
АЛГОРИТМ RSA

- Використовує два ключі: один для шифрування і один для дешифрування
- Ключ шифрування може бути розголошений (він стає "публічним ключем"), а ключ дешифрування зберігається в секреті (він стає "приватним ключем")
- Основу алгоритму RSA складає теорія чисел, а особливо теорія про прості числа



АЛГОРИТМ BLOWFISH

- Реалізує блочне симетричне шифрування
- Виконано на простих і швидких операціях: XOR, підстановка, додавання
- Незапатентований і вільно поширюється
- Реалізований у багатьох програмах, де не потрібна часта зміна ключа і необхідна висока швидкість шифрування / розшифрування



AES ПРОТИ DES

- **Ключова довжина:** AES підтримує ключі довжиною 128, 192 і 256 біт, що забезпечує вищий рівень безпеки. У DES ключ довжиною лише 56 біт, що робить його більш вразливим до атак перебору ключа.
- **Розмір блоку:** AES має фіксований розмір блоку 128 біт, тоді як DES має розмір блоку 64 біти. Більший розмір блоку дозволяє ефективніше шифрувати великі обсяги даних та запобігає певним атакам.
- **Швидкодія:** AES зазвичай пропонує більшу швидкодію порівняно з DES. У AES використовуються більш оптимізовані алгоритми та методи реалізації, що дозволяє шифрувати та розшифровувати дані швидше. DES має меншу швидкодію через менший розмір блоку та менш потужні алгоритми.
- **Безпека:** AES вважається більш безпечним алгоритмом порівняно з DES. DES, розроблений у 1970-х роках, був підданий криптоаналізу, і його ключова довжина 56 біт вважається недостатньою для сучасних вимог безпеки. AES був розроблений у 2001 році як преемник DES і пройшов ретельне аналізування і перевірку безпеки.
- **Розповсюдження:** AES отримав широке розповсюдження та застосування в різних сферах, включаючи комерційні системи, протоколи безпеки, програмне забезпечення та апаратні пристрої. DES використовувався широко протягом багатьох років, але зараз він вважається менш популярним через обмежену безпеку та недостатній розмір ключа.

AES ПРОТИ RSA

- **Тип шифрування:** AES є симетричним алгоритмом шифрування, що означає, що використовується один і той самий ключ для шифрування та розшифрування даних. RSA є асиметричним алгоритмом шифрування, що використовує пару ключів: публічний та приватний.
- **Застосування:** AES використовується переважно для шифрування секретних даних, таких як файли, повідомлення або комунікація між двома сторонами. RSA використовується для реалізації цифрових підписів, обміну ключами та інших протоколів, де необхідно забезпечити автентифікацію, цілісність та конфіденційність даних.
- **Ключова довжина:** У AES ключі можуть бути довжиною 128, 192 або 256 біт, що забезпечує високий рівень безпеки. RSA використовує ключі значно більшої довжини, зазвичай від 1024 до 4096 біт. Це пов'язано з його безпекою, більша довжина ключа забезпечує вищий рівень безпеки, але може вимагати більшого обчислювального ресурсу.
- **Швидкодія:** AES зазвичай пропонує більшу швидкодію порівняно з RSA. RSA залежить від складних математичних операцій, таких як піднесення до степеня та модульна арифметика, тому його швидкодія зазвичай нижча.
- **Безпека:** Якщо використовується правильно, як AES, так і RSA можуть бути безпечними алгоритмами шифрування. Однак, безпека RSA базується на складності факторизації великих простих чисел, тоді як безпека AES пов'язана з опіром до криптоаналітичних атак.

AES ПРОТИ BLOWFISH

- **Ключова довжина:** AES підтримує ключі довжиною 128, 192 або 256 біт, тоді як Blowfish підтримує ключі довжиною від 32 до 448 біт. Це означає, що AES може пропонувати більшу безпеку в контексті ключової довжини.
- **Розмір блоку:** AES має фіксований розмір блоку 128 біт, тоді як Blowfish має розмір блоку 64 біти. Більший розмір блоку у AES може забезпечити більшу безпеку та захист від певних атак, особливо при обробці великих обсягів даних.
- **Швидкодія:** Blowfish відомий своєю швидкодією, особливо при обробці великих обсягів даних. В той час як AES також швидкий, але в деяких випадках може мати трохи меншу швидкодію порівняно з Blowfish.
- **Безпека:** Як AES, так і Blowfish вважаються безпечними алгоритмами шифрування, що витримують значну криптоаналітичну атаку. Обидва алгоритми пройшли ретельні аналізи безпеки і є використовуваними в різних сферах.
- **Популярність та розповсюдження:** AES є більш популярним та широко розповсюдженим алгоритмом шифрування. Він є рекомендованим стандартом у багатьох галузях, включаючи комерційні системи та протоколи безпеки. Blowfish, хоча і використовується в деяких системах, не має такого самого рівня популярності та розповсюдження.

ВИСНОВКИ