|  |  |  |  |
| --- | --- | --- | --- |
| **Критерій** | **RSA** | | **DSA** |
| **Забезпечуючі механізми захисту** | **Шифрування, цифровий підпис** | | **Цифровий підпис** |
| **Довжина ключа** | **До 4096 біт** | | **До 1024 біт** |
| **ЗСП** | (N,P,Q): N – відкритий, P,Q(великі взаємнопрості) – конфіденційні (секретні).  ключі Еk≠Dk,(Еk – особистий, а Dk – відкритий - чи навпаки) | | Р – просте число,  і може змінюватися з кроком ,  q – просте число,    1 < g < p |
| **Алгоритм** | **1.**  **2.** =  **3.Обирається велике просте**  **4.Розв’язуємо рівняння**    **5.Отримуємо ()** | | **1. Великі прості q та p ((p-1) ділиться на q )**  **2.x – закритий ключ,**  **– відкритий ключ**  **3.Обараємо к взаємно просте з**  **(p-1).**  **4.якщо m – повідомлення**  **a,b – шифротекст**  **5.Розшифрування:** |
| **Тип** | **асиметричний, блоковий** | | **з використанням відкритого ключа** |
| **Час** | Час шифрування тексту залежить не тільки від довжини модуля перетворення, а й від розміру файлу, що шифрується. При тому ця залежність прямо пропорційна. | | Час вироблення ключової пари збільшується в залежності від збільшення модуля перетворення. |
| **Примітки** | Заснований на важкій задачі факторизації великих чисел; NP-повнота задачі не доведена і не спростована; один з перших асиметричних алгоритмів. | | Заснований на важкій задачі обчислення дискретних логарифмів в кінцевому полі; використовується тільки для підписання; довжина ключа обмежена 1024 битами; прийнятий як держ. стандарту США; застосовується для секретних і несекретних комунікацій; розробником є ​​АНБ. |
| **Стійкість** | Стійкість RSA базується на складності факторизації великих цілих чисел. | Криптографічна стійкість схеми DSA проти атак методом «грубої сили» в першу чергу залежить від розміру параметрів р і q. Успішна атака на параметр q можлива тільки в тому випадку, якщо зловмисник може обчислювати дискретні логарифми в полях Галуа GF з кількістю попередніх обчислень пропорційно. Однією з теоретично можливих атак на схему DSA є компрометація параметра к. | |
| **Висновки** | Таким чином, обидва алгоритми можна використовувати для того, щоб отримати ЦП, але ж RSA може використовуватись для шифрування інформації. Також, стійкість алгоритмів залежить від факторів, які не є спільними. DSA лежить в основі стандарту цифрового підпису, RSA є одним с перших асметричних алгоритмів, що був застосований для шифрування даних. | | |