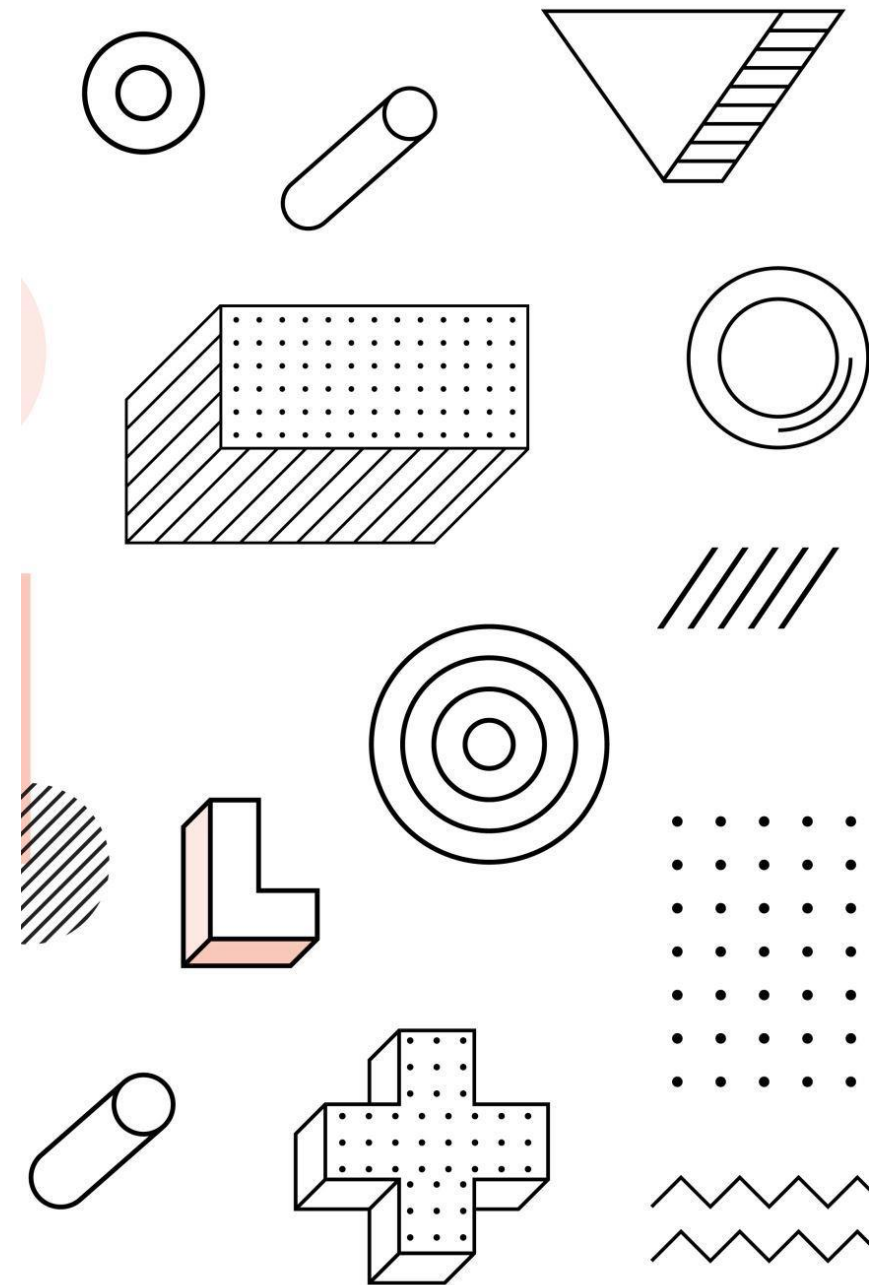


LOKI97

Підготував:

Кордюк Михайло, ПМІ-41



ІСТОРІЯ ТА РОЗРОБКА

LOKI97 було розроблено як одного з кандидатів у конкурсі AES з метою заміни шифру DES. Його створили Лорі Браун, Йозеф Пепржик і Дженніфер Себеррі у 1997 році. LOKI97 є частиною сімейства шифрів LOKI, що почалось з оригінального LOKI у 1991 році. Цей шифр має унікальні риси, які відрізняють його від інших претендентів AES.



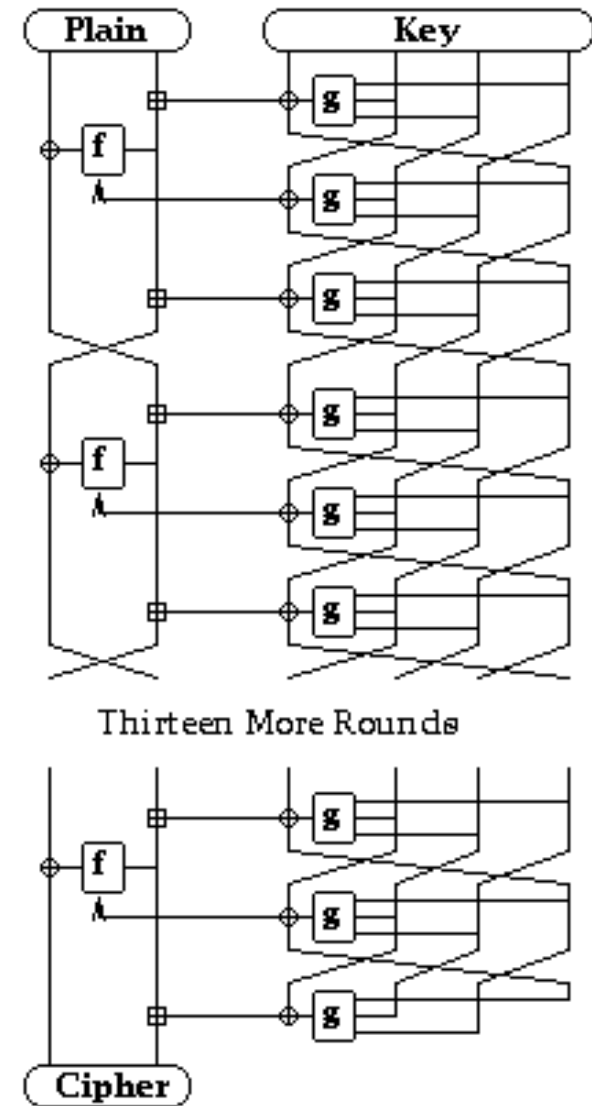
ПОРІВНЯННЯ З ІНШИМИ КАНДИДАТАМИ AES

- Під час конкурсу AES LOKI97 конкурував з іншими видатними алгоритмами, включаючи Rijndael, який в кінцевому результаті був обраний як стандарт. LOKI97 відрізнявся своїм підходом до структури шифру та ключового розкладу, але Rijndael продемонстрував кращий баланс швидкості, безпеки та гнучкості, особливо в обчислювально обмежених середовищах.



ОСНОВНІ ПРИНЦИПИ ТА СТРУКТУРА


LOKI97 - це блоковий шифр, який працює з блоками розміром 128 біт та використовує ключі довжиною 128, 192 або 256 біт. Він використовує структуру мережі Фейстеля з 16 раундами, використовуючи складну функцію, що включає етапи перестановки та заміни, натхненні шифром DES. Особливості конструкції LOKI97 забезпечують високий рівень безпеки проти традиційних криптоаналітичних атак.



АНАЛІЗ БЕЗПЕКИ ТА ВРАЗЛИВОСТІ

Хоча на момент створення LOKI97 вважався безпечним, подальший аналіз виявив вразливості до певних типів криптоаналітичних атак, таких як диференціальний та лінійний криптоаналіз. Ці вразливості були серед причин, чому LOKI97 не було обрано в якості AES. Згодом, дослідження цих слабких місць допомогли у розробці більш безпечних криптографічних алгоритмів.





Conclusions

ВИСНОВОК І СУЧАСНЕ ЗНАЧЕННЯ

LOKI97 залишається важливою частиною історії криптографії, надаючи уявлення про проектування та аналіз блокових шифрів. Хоча сьогодні він не використовується широко, вивчення LOKI97 може допомогти зрозуміти еволюцію стандартів шифрування та розвиток більш безпечних алгоритмів.