O‘QUVCHILARNI MA’LUMOTLARNI DESHIFRLASH ALGORITMINI QO‘LLASHGA O‘RGATISHNI SODDALASHGAN USULI

Shokir Bobobekov
Jizzax davlat pedagogika instituti
sh.r.bobobekov@mail.ru

Feruz Raxmonkulov
Jizzax davlat pedagogika instituti
feruz0123@jspi.uz

ANNOTATSIYA

Maqolada ma’lumotlarni deshifrlash uchun Feystel tarmog‘iga asoslangan simmetrik blokli shifrlash algoritmining soddalashtirilgan varianti taklif etilgan va ushbu algoritm yordamida hosil qilingan shifrmatnlarga mos keluvchi ochiq matnlar ikkita juftligining bitta kalit bilan shifrlash sikllari orqali o‘tish jarayonida o‘zgarishlarining o‘xshash emasligi tahliliga asoslanib, differentsial kriptotahlilni bir va to‘rt raunddan iborat bo‘lgan blokli shifrlash algoritmlariga qo‘llash va katta ehtimollikka ega bo‘lgan differentsiallarni aniqlash usuli tadbiqi keltirildi.
Kalit so‘zlar: Feystel shifri, kriptografiya, kriptotahlil, shifrlash, deshifrlash, shifrmatn, kalit.

ABSTRACT

The article proposes a simplified version of the Feistel network-based symmetric block encryption algorithm for data decryption, and analyzes the similarity of changes in the transition of two pairs of plaintext encryption cycles using one algorithm through one-key encryption cycles. based on the application of differential cryptanalysis to block encryption algorithms consisting of one and four rounds and the application of the method of detecting high-probability differentials.

Keywords: Feistel’s cipher, cryptography, cryptanalysis cipher, decryption, ciphertext, key.