ELEKTRON RAQAMLI IMZO ALGORITMLARINING QIYOSIY TAHLILI (RSA, ELGAMAL, DSA)

Yuldash Abdullayevich Kuralov
Toshkent viloyati Chirchiq davlat pedagogika instituti o‘qituvchisi
ykuralov89@mail.ru

ANNOTATSIYA

Mazkur ish kriptografiyaning muhim vazifalaridan biri - elektron raqamli imzoga bag’ishlangan. Elektron raqamli imzo (ERI) biror hujjatning muallifini bir qiymatli o’rnatish uchun zarur. ERI biror hujjat yoki shartnomaning haqiqiyligini ta’minlovchi oddiy imzoning analogidir. Ushbu ishda RSA, ElGamal va DSA algoritmlarining afzalliklari va kamchiliklari qarab chiqilgan

Kalit so‘zlar: shifrlash algoritmlari, elektron raqamli imzo, RSA, ElGamal, DSA.

COMPARATIVE ANALYSIS OF DIGITAL SIGNATURE ALGORITHMS (RSA, ELGAMAL, DSA)

ABSTRACT

This paper deals with one of the most important tasks of cryptography - the electronic digital signature. Electronic digital signature (EDS) is needed to uniquely establish the author of any document. EDS is the analog of a common signature that authenticates any document or contract. In this paper we look at the advantages and disadvantages of the algorithms RSA, ElGamal and DSA.

Keywords: encryption algorithms, electronic digital signature, RSA, ElGamal,DSA.