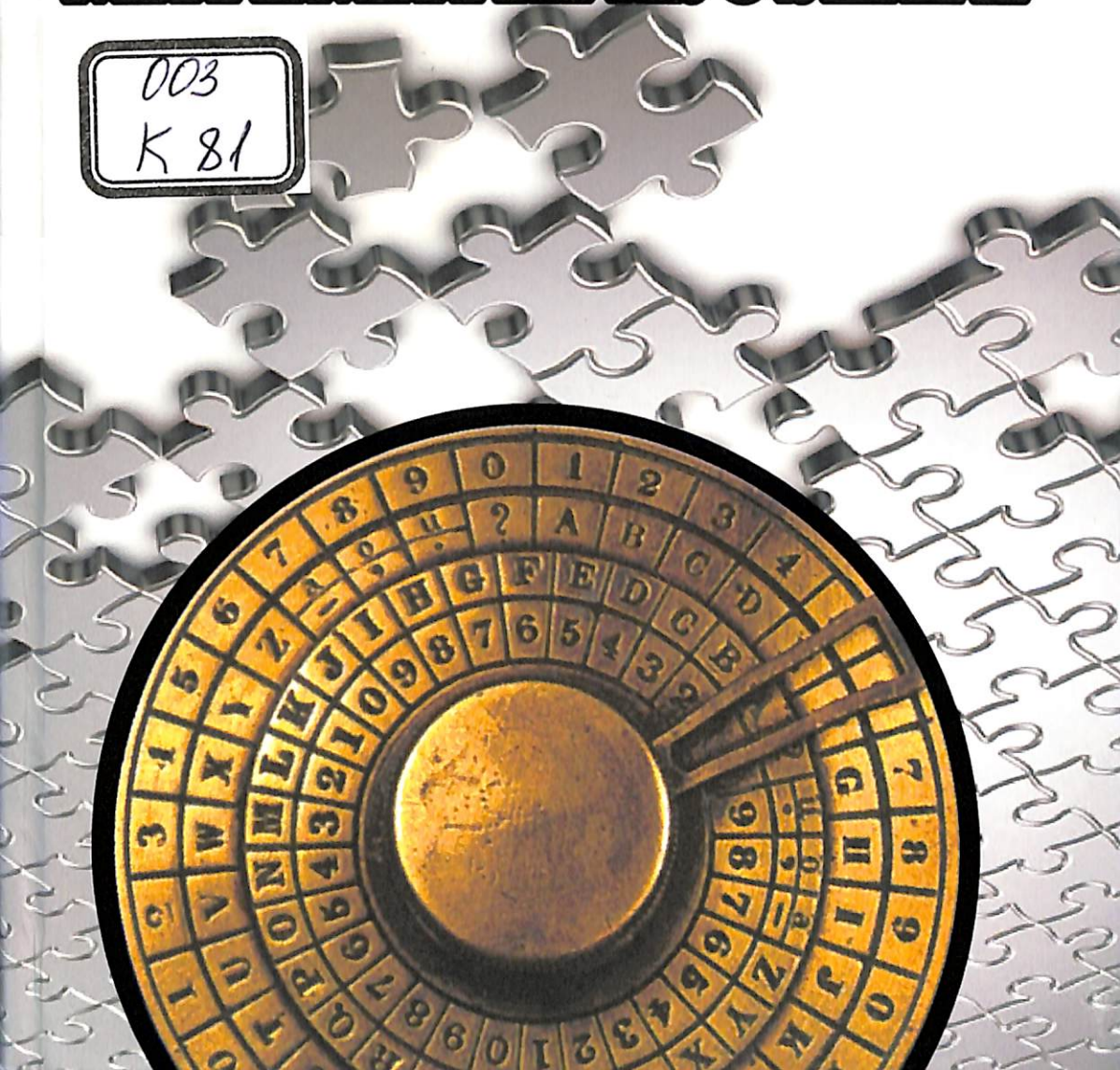
D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov,
O.P.Axmedova, I.U.Xolimtayeva

KRIPTOGRAFIYANING MATEMATIK ASOSLARI



O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI
VA KOMMUNIKASIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT
TEXNOLOGIYALARI UNIVERSITETI

KRIPTOGRAFIYANING MATEMATIK ASOSLARI

O‘quv qo‘llanma

Toshkent 2018

Mualliflar: Akbarov Davlatali Yegitaliyevich, Xasanov Po‘lat Fattoxovich, Xasanov Xislat Po‘latovich, Axmedova Oydin Po‘latovna, Xolimtayeva Iqbol Ubaydullayevna “Kriptografiyaning matematik asoslari”. O‘quv qo‘llanma. – Toshkent. TATU. 2018 – 208 bet

Ushbu o‘quv qo‘llanmada kriptografiya tarixi, kriptografiyaning asosiy matematik tushunchalari, ta’riflari, teoremalari hamda simmetrik va nosimmetrik kriptografik algoritmlarning matematik asoslari bayon etilgan.

O‘quv qo‘llanmada parametrli funksiyalar va ularning asosiy xossalari, diamatrisalar algebrasi va parametrli elliptik egri chiziqli funksiyalar hamda ular asosida ishlab chiqilgan kriptoalgoritmlar keltirilgan.

Ushbu o‘quv qo‘llanma Muhammad al-Xorazmiy nomidagi TATU axborot xavfsizligi va kriptografiya yo‘nalishida ta’lim olayotgan magistrlar uchun mo‘ljallangan. Shuningdek ushbu o‘quv qo‘llanmadan axborot xavfsizligi yo‘nalishida bakalavrlar tayyorlash jarayonida hamda kriptografiya yo‘nalishida ilmiy-tadqiqot olib borayotgan tadqiqotchilar, ilmiy xodimlar va soha mutaxassislari foydalanishlari mumkin.

O‘quv qo‘llanma Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti ilmiy-uslubiy kengashining qarori bilan chop etishga tavsiya etildi (2018 yil “____” “_____” “____”-sonli bayonnoma).

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, 2018

QISQARTMALAR

1.	AES (Advanced Encryption Standard) –	AQShning ma’lumotlarni shifrlash standarti.
2.	AQSh –	Amerika Qo‘shma shtatlari.
3.	GOST 28147-89 –	Rossiya Federasiyasining ma’lumotlar-ni shifrlash standarti.
4.	GOST R 34.10–94 –	Rossiya Federasiyasining diskret logarifmlashga asoslangan elektron raqamli imzo standarti.
5.	GOST R 34.10-2001 –	Rossiya Federasiyasining elliptik egri chiziqda diskret logarifmlashga asoslangan elektron raqamli imzo standarti.
6.	DES (Data Encryption Standard) –	AQShning ma’lumotlarni shifrlash standarti.
7.	DSA (Digital Signature Algorithm) –	AQShning diskret logarifmlashga asoslangan elektron raqamli imzo algoritmi.
8.	EC-DSA-2000 (Elliptic Curve Digital Signature Algorithm) –	AQShning elliptik egri chiziqda diskret logarifmlashga asoslangan elektron raqamli imzo algoritmi.
9.	EC-KCDSA –	Koreyaning elliptik egri chiziqda diskret logarifmlashga asoslangan elektron raqamli imzo algoritmi.
10.	EC-GDSA –	Germaniya Federativ Respublikasining elliptik egri chiziqda diskret logarifmlashga asoslangan elektron raqamli imzo algoritmi.
11.	EKUB –	Eng katta umumiy bo‘luvchi.
12.	FEAL (Fast Data Encryption Algorithm) –	Yaponiya ma’lumotlarni shifrlash algoritmi.
13.	IDEA (International Data Encryption Algorithm) –	Xalqaro ma’lumotlarni shifrlash algoritmi.
14.	KROM –	Kalitlarni ro‘yxatga olish markazi.

15.	NIST (National Institute of Standards and Technology) –	Standartlar va texnologiyalar milliy instituti
16.	MShA –	Ma’lumotlarni shifrlash algoritmi.
17.	PTKK –	Psevdotasodifiy ketma-ketlik.
18.	RSA –	Rayvest-Shamir-Adleman algoritmi.
19.	XOR –	2 modul bo‘yicha qo‘shish.
20.	O‘z DSt 1092:2005, O‘z DSt 1092:2009 –	O‘zbekistonning daraja parametri muammolarining murakkabligiga asoslangan elektron raqamli imzo bo‘yicha davlat standartlari.
21.	ERI –	Elektron raqamli imzo.
22.	ERIA –	Elektron raqamli imzo algoritmi.
23.	EECh –	Elliptik egri chiziq.