**O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI.**

**Fan :** Kriptografiya

**Kafedra** : Kriptologiya

**Amaliy ishi**

**MAVZU: Psevdotasodifiy sonlar generatorini va uning dasturiy ta’minotini yaratish**

**Guruh : 713-19**

**Bajardi : Norov Azizbek**

**Tekshirdi : Mardiyev U**

**Toshkent-2021**

**12- Amaliy ish**

**Mavzu: Psevdotasodifiy sonlar generatorini va uning dasturiy ta’minotini yaratish**

**Ishdan maqsad**: Psevdotasodifiy sonlar generatorlar haqida bilim ko‘nikmalarga ega bo‘lish.

**Nazariy qism**

DES shifrlash algoritmi yordamida psevdotasodifiy ketma-ketliklarni generasiya qiling. Quyidagi kongruent generatorlarni amalga oshirish

𝑥𝑛+1 = (𝑎𝑥𝑛 + 𝑏)𝑚𝑜𝑑 𝑚;

𝑥𝑛+1 = (𝑎𝑥𝑛2 + 𝑏𝑥𝑛 + 𝑐)𝑚𝑜𝑑 𝑚;

𝑥𝑛+1 = (𝑎𝑥𝑛3 + 𝑏𝑥𝑛2 + 𝑐𝑥𝑛 + 𝑑)𝑚𝑜𝑑 𝑚;

Bu yerda

𝑥𝑛 −ketma-ketlikning 𝑛 hadi,

𝑥𝑛+1 −ketma-ketlikning navbatdagi hadi,

𝑎, 𝑏, 𝑐, 𝑑- kongruent generator parmetrlari, m -modul.

**Topshiriq**

Quyida keltirilgan variantlar bo‘yicha kongruent generatorlar asosida ketmaketliklarni hosil qiling va davrini hisoblang.

|  |  |
| --- | --- |
| **№** | **Generator parametrlari** |
| 22. | a=12, b=7, c=8, d=10, m=19 **X0=22** |

**𝑥𝑛+1 = (𝑎𝑥𝑛 + 𝑏)𝑚𝑜𝑑 𝑚;** quyidagi funksiya asosida davrni topish uchun hisoblashni boshlaymiz.

𝑥0=22

**𝑥1 = (12\*22+ 7)𝑚𝑜𝑑 19= 5** 𝑥5 = (12\*11+ 7)𝑚𝑜𝑑 19=6

𝑥2 = (12\*5+ 7)𝑚𝑜𝑑 19=10 𝑥6 = (12\*6+ 7)𝑚𝑜𝑑 19=3

𝑥3 = (12\*10+ 7)𝑚𝑜𝑑 19=13 **𝑥7 = (12\*3+ 7)𝑚𝑜𝑑 19=5**

𝑥4= (12\*13+ 7)𝑚𝑜𝑑 19=11

**𝑥1 = 𝑥7=5** 6 tada takrorlandi.

Endi esa kvadrat funksiyaga o’tamiz. Bunda ham shu tariqa hisoblab takrorlanishni aniqlaymiz.

**𝑥𝑛+1 = (𝑎𝑥𝑛2 + 𝑏𝑥𝑛 + 𝑐)𝑚𝑜𝑑 𝑚;**

𝑥0=22

𝑥1 = (12\*222 + 7\*22+ 8)𝑚𝑜𝑑 19=4 𝑥4= (12\*82 + 7\*8+ 8)𝑚𝑜𝑑 19=15

𝑥2= (12\*42 + 7\*4+ 8)𝑚𝑜𝑑 19=0 𝑥5= (12\*152 + 7\*15+ 8)𝑚𝑜𝑑 19=1

**𝑥3= (12\*02 + 7\*0+ 8)𝑚𝑜𝑑 19=8** **𝑥6= (12\*12 + 7\*1+ 8)𝑚𝑜𝑑 19=8**

**𝑥3 = 𝑥6=8** 3 tadan keyin takrorlandi.

Endi esa 3 darajali funksiyani ham xuddi shu tarzda hisoblaymiz.

**𝑥𝑛+1 = (𝑎𝑥𝑛3 + 𝑏𝑥𝑛2 + 𝑐𝑥𝑛 + 𝑑)𝑚𝑜𝑑 𝑚;**

𝑥0=22

**𝑥1 = (12\*223 + 7\*222 + 8\*22+10)𝑚𝑜𝑑 19=3**

**𝑥2 = (12\*33 + 7\*32 + 8\*3+10)𝑚𝑜𝑑 19=3**

**𝑥1 = 𝑥2=3** 1 tadan keyin takrorlandi.