

# Xesh funksiyalar.

1. Xesh jadval va xesh funksiya nima ?
2. Xesh funksiyalarning qanday turlari mavjud?
3. Oddiy xesh funksiya strukturasi va unga doir misollar keltiring ?
4. Kriptografik xesh funksiya strukturasi va unga misollar keltiring ?
5. Polinimal xesh funksiya strukturasi izohlang
6. Kiruvchi ma'lumotlarni polinimal xesh funksiya yordamida xeshlang.
7. Quyidagi tushunchalarni izohlang, kodlash, shifrlash, tekis kodlash, noteks kodlash, xesh jadval, xesh funksiya, kriptografiya, kolluziya muammosi.
8. “ Algoritm va ma'lumotlar strukturasi” matnini Adler-32, SHA-1, MD-4, MD-5, Tiger xesh funksiyalari yordamida xeshlang.
9. Quyidagi keltirilgan md-5 xesh funksiyasi orqali chiquvchi ma'lumotni, kirish qiymatini aniqlang.

```
7650d3efe9d32071f601e9d148767d26
```

10. Quyidagi dasturni tahlil qiling.

```
#include <iostream>

#include <string.h>

using namespace std;

int main()

{char a[100];

cout<<"So'zni kiriting: = ";

cin.getline(a,100);

cout<<"Shifrlangan kalit";

for(int i=0,j=strlen(a)+67; j<=strlen(a),i<=strlen(a);i++,j=j+3)

cout<<char (j)<<j<<(int)a[i]+55+122*2<<char(j);

cout<<endl;

main();

return 0;
```

```
}
```

**11.** Quyidagi dasturni tahlil qiling va xesh funksiya turini aniqlang.

```
#include <iostream>
```

```
using namespace std;
```

```
int main()
```

```
{
```

```
    int i, x;
```

```
    char str[100];
```

```
    cout << " Matnni kiriting: ";
```

```
    cin >> str;
```

```
    cout << " 1 - Matnni shifrlash. \n";
```

```
    cout << " 2 - Shifirni matnga qaytarish. \n"; cin >> x;
```

```
    switch(x)
```

```
    {
```

```
        case 1:
```

```
            for(i = 0; i < 100; i++)
```

```
            {
```

```
                if(str[i] >= 33 and str[i] <= 126){
```

```
                    str[i] += i*i%2+7;
```

```
                }
```

```
            }
```

```
            cout << " \n Shifrlangan matn: " << str << endl;
```

```
            break;
```

```
        case 2:
```

```

    for(i = 0; i < 100; i++)
    {
        if(str[i] >= 33 and str[i] <= 126){
            str[i] -= i*i%2+7;
        }
    }

    cout << " \n Shifirni matnga qaytarish: " << str << endl;
    break;

    default:

        cout << " \n 1 yoki 2 ni tanlang! \n ";
    }

    main();

}

```

## 12. Polinimal xeshlash algoritmi strukturasini izohlang.

```

#include <iostream>
#include <string.h>
using namespace std;

long long Heshlash(char s[])
{
    long long h = 0;
    int base = 37;
    for(int i=0; i<=strlen(s); i++)
    {
        h = h* base + s[i] - 61 +1;
    }
}

```

```

    }
    return h;
}

int main()
{
    char s[100];

    for(int i=1; i<10; i++)
    {
        cin.getline(s,100);
        cout<<s<<" "<<Heshlash(s);
        cout<<endl;
    }
}

```

13. Quyidagi jadvalni tahlil qiling.

	Xeshlanadigan matn uzunligi	Kirish bloking uzunligi	Xesh qiymat uzunligi	Har bir blokni xeshlash qadamlari soni
<b>GOST R 34.11-94</b>	Ixtiyoriy	256	256	19
<b>MD 2</b>	Ixtiyoriy	512	128	1598
<b>MD 4</b>	Ixtiyoriy	512	128	72
<b>MD 5</b>	Ixtiyoriy	512	128	88
<b>SHA-1</b>	$<2^{64}$	512	160	80

14. Online xesh kalkulyatori yordamida kriptografik turli xil hesh funksiyalardan foydalanib, Ism, familiyangiz, va sharfingizni xeshlang.

<https://md5calc.com/hash/md5>

15. Online xesh kalkulyatori yordamida kriptografik turli xil hesh funksiyalardan foydalanib xeshlang va xeshlangan ma'lumotni asliga qaytaring.

16. Polinimal xesh funksiya dasturini tuzing.

17. Oddiy xesh funksiya dasturini tuzing.

**18.** Kriptografik xesh funksiya dasturini tuzing.

**19.** Xesh funksiylarning maqsadi va ularni amaliyotga tadbir'i.

**20.** Xesh funksiylarning murakkabligini tahlil qiling. Yaxshi xesh funksiya qanday talablarga javob berishi lozim?