Kriptografik protokollar fanidan oraliq nazorat savollari

1-variant

1. Kriptografik protokollarni zaifligi
2. Maxsus algoritmlar, ya’ni ERI protokollari asosida hujjatlarni imzolash
3. Fiat-Shamir protokoli
4. Brikell va MakKarli sxemasi
5. RSA kriptotizimiga asoslangan protokol

2-variant

1. Kriptografik protokollar va ularning xavfsizligiga qilinadigan asosiy hujumlar
2. Parol bo‘yicha autentifikasiyalashga hujumlar
3. Fiat-Shamir va Feyga Fiat-Shamirning farqi
4. Qoldiq haqidagi Xitoy teoremasiga asoslangan sirni taqsimlash sxemasi
5. Shnorr sxemasi

3-variant

1. Simmetrik kriptotizim va uchinchi shaxs ishtirokidan foydalanib, hujjatlarni imzolash protokoli
2. Lamport protokoli. Parol mustahkamligini miqdoriy baholash
3. Gillu-Kiskate protokoli
4. Lagranj interpolyasion ko‘phadiga asoslangan Shamir sxemasi
5. Sirni taqsimlashning bo‘sag‘ali sxemalari

4-variant

1. Ochiq kalitli kriptografiyadan foydalanib, hujjatlarni imzolash
2. Savol-javob» tamoyiliga asoslangan autentifikasiyalash protokollari
3. Okamoto protokoli
4. Fiat-Shamirning autentifikasiyalash protokoli
5. Brikell va MakKarli sxemasi