1. Kriptologiya tushunchasi nima va u qanday asosiy yo‘nalishlardan iborat?
2. Kriptografiya va kriptoanaliz o‘rtasidagi asosiy farqlar nimada?
3. Kriptoanalizning asosiy maqsadi va vazifalari qanday?
4. Zamonaviy kriptografiyaning asosiy yo‘nalishlari va qo‘llanilish sohalari qaysilar?
5. Simmetrik va asimmetrik kriptografiya orasidagi asosiy farqlar nimalarda namoyon bo‘ladi?
6. Zamonaviy dunyoda kriptologiya qaysi sohalarda katta ahamiyat kasb etadi?
7. Kriptografik tizimlarning samaradorligi qanday omillarga bog‘liq?
8. Kriptoanaliz usullari qanday bosqichlardan iborat va ular qanday amalga oshiriladi?
9. Kriptoanaliz nima va uning asosiy maqsadi qanday?
10. Kriptotizimlarga qarshi hujumlarning asosiy turlari qanday?
11. Tanlangan ochiq matn (chosen plaintext attack) asosidagi hujum usullarini qanday amalga oshirish mumkin?
12. Tanlangan shifr matn (chosen ciphertext attack) asosidagi hujum usullarining o‘ziga xos xususiyatlari qanday?
13. Zamonaviy kriptotizimlarda kriptoanalizning qanday ahamiyati bor?
14. Simmetrik va asimmetrik kriptotizimlarga qarshi hujumlar o‘rtasidagi asosiy farqlar nimada?
15. Kriptoanaliz va kriptografiya o‘rtasidagi bir-birini to‘ldiruvchi munosabat qanday amalga oshadi?
16. Klassik shifrlarga misol keltiring va ularning asosiy xususiyatlarini tushuntiring.
17. Sezar shifri qanday ishlaydi va unga qarshi kriptoanaliz qanday amalga oshiriladi?
18. Vijiner shifri nima va unga qarshi kriptoanaliz qanday amalga oshiriladi?
19. Matnning harf chastotasini tahlil qilish klassik shifrlarni buzishda qanday qo‘llaniladi?
20. Klassik shifrlarga qarshi bruteforce (qo‘pol kuch) usuli qanday ishlaydi?
21. Sodda klassik shifrlar va zamonaviy kriptografik algoritmlar o‘rtasidagi asosiy farqlar nimada?
22. Kriptografik bardoshlilik tushunchasi nima va uning asosiy xususiyatlari qanday?
23. Kriptografik algoritm bardoshliligi qanday omillarga bog‘liq?
24. Algoritmning bardoshliligini baholash uchun qaysi mezonlardan foydalaniladi?
25. Simmetrik va asimmetrik kriptografik algoritmlarning bardoshliligini qanday taqqoslash mumkin?
26. Zamonaviy kriptografik algoritmlarning bardoshliligini oshirish uchun qanday usullar qo‘llaniladi?
27. Matematik murakkablik kriptografik bardoshlilikka qanday ta’sir qiladi?
28. Algoritmlarning bardoshliligini baholash uchun statistik testlar qanday qo‘llaniladi?
29. Hisoblash murakkabligi nazariyasi nima va uning asosiy maqsadi qanday?
30. Algoritmning hisoblash murakkabligi qanday tushuntiriladi va qanday o‘lchanadi?
31. Kriptografik algoritmlar hisoblash murakkabligiga nisbatan qanday talablarni qondirishi kerak?
32. Diskret logarifmlash muammosi qanday murakkablik darajasiga ega?
33. Algoritmning xotira murakkabligi va hisoblash tezligi o‘rtasidagi bog‘liqlik qanday?
34. Hisoblash murakkabligi nazariyasi kriptoanaliz va kriptografiyada qanday amaliy ahamiyatga ega?
35. Kriptoanalizning universal usullari nima va ular qanday holatlarda qo‘llaniladi?
36. Qo‘pol kuch (bruteforce) usuli qanday ishlaydi va uning afzalliklari hamda kamchiliklari qanday?
37. Xesh-funktsiyalarning kolliziyasini topish kriptoanalizda qanday ahamiyatga ega?
38. Universal usullar yordamida kriptotizimlarning zaif tomonlarini qanday aniqlash mumkin?
39. Universal usullarni qo‘llashda hisoblash resurslari va vaqt murakkabligi qanday baholanadi?
40. Zamonaviy texnologiyalar universal kriptoanaliz usullarining samaradorligiga qanday ta’sir qiladi?
41. Pollard rho usuli qanday ishlaydi va u qaysi muammolarni yechishda qo‘llaniladi?
42. Chiziqli kriptoanaliz usuli nima va u simmetrik blokli shifrlarga qanday ta’sir qiladi?
43. Chiziqli kriptoanalizning asosiy maqsadi qanday va u qanday hujumlar uchun samarali?
44. Simmetrik blokli shifrlarda chiziqli kriptoanaliz usulini qo‘llash uchun qanday ma'lumotlar talab etiladi?
45. Chiziqli aproksimatsiya nima va u chiziqli kriptoanalizda qanday rol o‘ynaydi?
46. Chiziqli kriptoanaliz usulida shifr qismlari qanday tahlil qilinadi?
47. Chiziqli kriptoanaliz usuli qanday algoritmlarda samarali bo‘lishi mumkin?
48. Differensial kriptoanaliz usuli nima va u simmetrik blokli shifrlarga qanday ta’sir qiladi?
49. Differensial kriptoanaliz usuli qanday shifrlash tizimlarida samarali bo‘lishi mumkin?
50. Differensial tahlil va chiziqli tahlil o‘rtasidagi asosiy farqlar nimalarda?
51. Differensial kriptoanalizda shifrlangan matnlar o‘rtasidagi farq qanday tahlil qilinadi?
52. Differensial kriptotahlilda orttirmalar qanday tanlanadi va ular kriptoanalizda qanday yordam beradi?
53. Simmetrik blokli shifrlarda differensial kriptoanaliz usulini qo‘llash uchun qanday maxsus shartlar kerak?
54. Chiziqli-differensial kriptoanaliz usuli nima va u simmetrik blokli shifrlarga qanday ta’sir qiladi?
55. Chiziqli-differensial kriptoanaliz usulining asosiy maqsadi va afzalliklari qanday?
56. Chiziqli kriptoanaliz va differensial kriptoanaliz o‘rtasidagi asosiy farqlar nimalarda?
57. Algebraik kriptoanaliz usuli nima va u simmetrik blokli shifrlarga qanday ta’sir qiladi?
58. Algebraik kriptoanalizda polinomial tenglamalar qanday rol o‘ynaydi?
59. Simmetrik blokli shifrlarda algebraik kriptoanaliz usulini qo‘llash uchun qanday algebraik tuzilmalar kerak?
60. Shifrlash tizimlaridagi algebraik munosabatlar qanday aniqlanadi va ular kriptoanalizda qanday qo‘llaniladi?
61. Integral kriptoanaliz usulining mohiyati nimadan iborat?
62. Integral kriptoanalizning asosiy maqsadi qanday va u qanday shifrlash tizimlarida samarali bo‘lishi mumkin?
63. Simmetrik blokli shifrlarda integral kriptoanalizni amalga oshirish uchun qanday ma'lumotlar kerak?
64. Integral kriptoanaliz usulini qo‘llashda algoritmlar bardoshliligi qanday baholanadi?
65. Apparat xatoliklarni generatsiyalashga asoslangan kriptoanaliz usuli nima va u qanday ishlaydi?
66. Simmetrik blokli shifrlarda apparat xatoliklarni generatsiyalash qanday qilib kriptoanalitik hujumga aylanishi mumkin?
67. Apparat xatoliklari qanday ko‘rinishlarda bo‘lishi mumkin va ularning kriptografik tizimga ta’siri qanday bo‘ladi?
68. Asimmetrik kriptotizimlar nima va ular qanday ishlaydi?
69. Faktorlash muammosi qanday ta’riflanadi va nega asimmetrik kriptotizimlarda uni yechish qiyin?
70. Faktorlashning murakkabligi kriptoanalizda qanday rol o‘ynaydi?
71. Asimmetrik kriptotizimlarda faktorlash muammosining murakkabligini aniqlashning qanday metodlari mavjud?
72. RSA kriptotizimida faktorlashning ahamiyati qanday va u qanday hujumlar uchun xavf tug‘diradi?
73. Asimmetrik kriptotizimlarning xavfsizligi va faktorlashning murakkabligi o‘rtasidagi bog‘liqlik qanday?
74. Asimmetrik kriptotizimlarda faktorlashni amalga oshirish uchun qanday klassik va zamonaviy usullar qo‘llaniladi?
75. Diskret logarifmlash muammosi nima va asimmetrik kriptotizimlarda qanday rol o‘ynaydi?
76. Diskret logarifmlashning murakkabligi kriptoanalizda qanday ta’sir qiladi?
77. Diskret logarifmlash muammosini yechish uchun klassik va zamonaviy usullar qanday qo‘llaniladi?
78. Pollard's rho algoritmi diskret logarifmlashni yechishda qanday samaradorlikni ko‘rsatadi?

Berilgan sonni, berilgan modul bo‘yicha teskarisini topish.

1. ;
2. ;
3. ;
4. ;
5. ;

Quyida keltirilgan RSA shifrlash algoritmi yordamida shifrlangan matnni rasshifrovka qiling.

1. C= 177611, N= 474473, e= 37;
2. C= 259064, N= 360329, e= 37;
3. C= 361708, N= 381923, e= 43;
4. C= 128383, N= 333511, e= 43
5. C= 116533, N= 161803, e= 43
6. C= 103982, N= 381847, e= 53
7. C= 31044, N= 37403, e= 53
8. C= 33386, N= 285143, e= 79
9. C= 388236, N= 481391, e= 77
10. C= 66013, N= 267181, e= 79
11. C= 112856, N= 158381, e= 79
12. C= 291331, N= 442661, e= 77
13. C= 26425, N= 173317, e= 103
14. C= 161774, N= 286837, e= 103
15. C= 101672, N= 239663, e= 103
16. C= 449599, N= 525851, e= 239
17. C= 211372, N= 656099, e= 239
18. C= 536213, N= 654583, e= 237
19. C= 82605, N= 88303, e= 235
20. C= 172513, N= 279373, e= 235