Асиметрична криптографія
Лабораторна робота № 3

Криптосистема Рабіна
Атака на протокол доведення знання без розголошення

Мета
Ознайомлення із криптосистемою Рабіна та особливостям її реалізації.
Ознайомлення з криптографічними протоколами взагалі та протоколами доведення знання без розголошення зокрема. Ознайомлення із перевагами, недоліками та особливостями реалізації різних криптографічних протоколів. Аналіз наведеного протоколу; реалізація атаки на цей протокол.**Постановка задачі**
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжиниr= 2, 3,4, 5, а також довжини 10-20 знаків.Зашифруватиобраний відкритий текстшифромВіженера з цими ключами.
2. Підрахувати індексивідповідностіrIдлявідкритого тексту тавсіходержанихшифротекстіві порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданийшифртекст(згідно свого номеру варіанта).Зокрема, необхідно:–визначити довжину ключа, використовуючи або метод індексів відповідності, абостатистику співпадіньDr(на вибір);–визначити символи ключа, прирівнюючи найчастіші літери у блоці донайчастішої літери у мові;–визначити символи ключа за допомогою функціїM(g)i;–розшифрувати текст, використовуючи знайдений ключ; в разі необхідностіскорегувати ключ

Хід роботи
Булот реалізовано шифрування, нажаль невалося релізувати розшифрування та підписи через проблему з падінгом. Проблеми з'являлися на кожному кроці, найкращий результат, що було досягнуто при розшифруванні то це розшифрування але в не те що потрібно.
Було написано код для маленької програмки, яка генерувала випадкове значення t за модулем n, потім його підносили до квадрату, отримували значення y і його надсилали серверу. З допомогою отриманого значення z від сервера й нашого t, шукали по суті за Ферма дільники n, тобто особистий ключ p і q, як НСД(t-+z, n). За невелику кількість спроб вдавалося знайти, потрібна кількість спроб зазвичай від двох до чотирьох

Приклад реалізованої атаки
Атака на протокол доведення із нульовим розголошенням: n =
89000FDD895B54EEC8BDD89EA9672250E737D733841BBC28D1A8EE9B234CBBF13D2825757D104452F9
211186A38F2ABE8477077068D2CC6486C28609D0FCC7B8F9E71F1990451813A3212AEF5F62826AF6AFE4
D36C63CEE7FC323829F5C799E873CD42DD04D581AF0A7DAD193340709482D92EF6E9701BB2ADEEEFE
7B05E611E8984AB4D53C859025CB8073D539AEDB6AD03CBA9FF325214BB08ADE259E9FDC11FB534D
589554939E39702144A52573B3F0939AC99DDB21D4A8B09D9BDC9AAD2D1542A3A2FBA051611017118C
AFB8452B1E760F9A2F83E0BC26840C908A1CD6CBF4D5E128E2204CADBE7CD5862E429CFFB0860BCC
78A3B907996B4162552E655 Спроба 1 Надіслати серверу y =
0x646770cff69a17faff52dff224f2994148ac5e4dddc7678e9e98afebdf896c1e1024ddb0e13ca1a9c66b990fbea1e7d
ae9e56bc7974b9ce0302043e179f0e191d2105a082da23ca6f17492d201c3dbb4c4b9f7262cb4624f867ff06e864af14
b8133cf49a6707b751839d9f6b59f5282aa4de30fb507cd276ae31af8219ad6be06853188b4633673a6de6452b6b41e
0e29acda08928a6bc547215113ae299265cdf9e5ddebd70d7bd6d240ea6839c78903be8a37be2233e284a42d0ef26a
b44dc2667b8012db52e11e7237c75c9eee27d18a99c71a3e2a528453559b582b7bc033b043d61c00c60dfd4fdfbbcf2
ab37267dbd415c2d58a20c8c95fc1124e8d26 Ввести отримане z:
FE8C8097A012340927FEEB4C68850287978E45585C37D1A7032576A44D5070E0B0004F5AEFA0DF25CF51
9125BA16626DD8101ECD69128E0DA8A0FD13A47C3D36844E34C83163E90799994C7D5E4939AE40E0D9
B7062F02C025E33B90AB1FAE05D434B52487998948E059276EE414D4E07881CE6C9FA0FA7F091D3C5C1
DFB8D049A0FB97BBA15205754B0A5BC17008421DF1FF68626AE73A2E5E55BB62B0E6EFB7F611877715
9D09D8A38822957DC59202902C92AC4516E61B93A6E0F86284F0117DC10903F5BE3B7D82C52058A14B7
3FC4F50D15728470DAD89FF3A1537109C7AFAD8FC7FEC9651482FC03823D1F2EC37CF650A93A47DF7A
83AC9F947FE22A8 Не пощастило Спроба 2 Надіслати серверу y =
0x5714db772a334442c25e2d3b1adfa5ffe86bd99579fe338bbee8b8e4d921db9052755af995c2ccac4dda017cf8cfd8
727b729a87adcdd9eaf612e0dcab4f12637a07e72f060b81979d45d22d9bcb6bb35f5c92bcc341108fcda3588cebcc3
5bc7006f336c7e5135a26118a843465dc1141b03335426d518cd1d66057866305b25f322155d2b2f9bc64c540e4fed

8000922ae16e0df48a1fac1c205e6b82c788447b1c217f3e758763e6001e100d578843f800a16c5540beb68856c4f22
4858263094a145eecbcc181080e64facb240b289e0ed6dfd03e4c72192e7e4aaee65999104ee7162b9569a3e0333eab
11a6d0d8d435246fd6cca3b720cb8f77772f840 Ввести отримане z:
5831D94102A9A0BBC7489708C87AE389E8E671B7C3BE6BC3FB76ACE9EDCC5D32034121F2E9B7EBB2
ADD4144DF8F9F59253BD90EF2351F0D9E63C2D42FF9C4E978FAD1B30F6D19B1C6E88F22D1A262E1921
6B8FB8E81DD236F3112D044BF8379A21E2F817489013776C7FE3435BD16A735244E35314DD0E9FA8214E
A9EEE1446A997F3CEF532813B8D782710241FD9C56033F4A5AEC4CAF9D9017C01C969016BE0740A56F
CD6A0E94B018C43FFEB68FC824D8248C061E85F2FA17ABC11707C027CDD340E0493FF392D7C1978C96
6F6C9EEDA7B08AB2A7CED903F7A2342AA232D41123AD6D3F6EB34F6A76C627837D42556106C897E2D
E7E0317BF39C8F2A38D3B Не пощастило Спроба 3 Надіслати серверу y =
0x950f519b56cd7e100800b989c2eedc227d17d36c99667c6f4032adcbb5708736e86ddfa5940d21b7b333d9607238
ff73f9fa6308506c71fce23982898bc6b6c01e91c233d81b94e939fc239bbedbea16c2f885a28d0cc107147c10a57dcd
702830945f5768a51e37e6a78f6fffbb809b1633e45cef6fcdf7ed21dba885ae50695de7c02a0a00323db0c001b79e52
7f68e9360091c5eacf2cd8b8af8aa32a7d74407b556a5246f62908636eb837ac6675cefdc14182a2711883b390c98b0
1300fcbe2a8ae850ffd79a630efde6fc6f27fb956d69b6d0ad15823fff281090b5094527baad4cab8e911b321ac7356da
6719b1621458fb5646100e54d07e66587da Ввести отримане z:
246E87B4F89F87165B9BB7823DA14527FDF99B9922A22C19B3C8E45C43862D1DF84ECA1FF582806CCF
CC23602BED1B939E25695C81D260490E8AFDE6106027B8CA83A5E404D75E97E9C2E216B23FAC898A88
4007CC83C2C8D65F1002449780BADF439FAB38BEB7C6EF46C17437D51A6C1DA1B876536593A9959AA
C9171A7926CB4CEC1622A37CCECDAF7D28750F5E30E6927F0B149613D1B5F7D27DAC1498ED37FFC2D
7E17AEE45B46012E2760CD039EE6818D43FB7C43D47C1F739AA9D1FFF62B704276E2DE5C7509DEC6F6
30656EFA0CAF073E65C9BC39C937D18F0F62D2C2C8837A099B29629F813C1ABA0704DF27FE99B68AEC
FBFBDCC7BF22DE6D6E34DF Не пощастило
Спроба 4 Надіслати серверу y =
0x7b94055d2371a3c90b85af47fa86a91786442fdfe8c25193c726a7ab9cf77132d27538dcf3013dd8209e69f236493
8389656ad088e32d37a33cbd25ff1cb93f15a592e316433aeb06ce440d538b6ea279b19a73419f57466a8ccdf6fcbc9
d0c73d90bd26bb7229c6263001ee308b26045a5ea9eb7016c98d9e2496c08b47bd80ebb49ae401130a20ecd88f2c16
3acfd305fb730fe8adf5e89305b15430478e8d5ea4cd4b661ff0f29ecbabe3b7486462216c3c93538730b52b3975078
0a65f58fd5cd91e1c8f962558d6325ba7d9724c4dc2765d882292459ac5be7e7f9b8a4adaa94d9284e614c0ada33712
aeceacc0874131b2ee308283d6a608bd81a3da5c Ввести отримане z:
4D34CCE8A58990C6247111B672AE2F8A0F0F0C2A527D3B15C4CC637CA737BC3D19EC90CF50CF3F047
272BABFA4C81E7013B06C58FCFF8A16848C2AD349314912F803A2D97EDCD1468904EE67C236921B8D2
49B494CD9D0CCD4FD5A314E731C3C72826F852B8249197183E83EBAE9FE93F28CDCEE636C20425356B
102A9F99835FBD90587374FA4FA668F97146AFDB54C31305150C2A4E9D10CA600DE812A5E53B0CDBD
DAADFB8DC1BC74795F97FE47B4D62B98C0C999BB275DAA0F52CE3CF12D16480962CBC63CB243E7A7
D298F087DF1BEB49FC5757CF239E682E1843968951D4E34304B63F42D9E57E264A6C2E3C0A0FE108F1C
0DB2B219C362199801EDB6F Знайдено p =
0x894a4e482ca37ae2fd6e2f5da68d5ae5f240aa0b2215c3cefced9a8b1d1af68bdcc2abf7f1e2906e8976957decc47a2
34e45fd0306a779a99b697b5504bf6f4d3f43ecc7f8ab4812841781181e1013e3ba830dad6e4750b3a7696b5637959
de9594c9c74b3e7791b7c909f9fc6a4e53dad045b7367613ce83a3e6f5ffb13493f І маємо q =
0xff758f726a73e1845238b1c54f65317b8ddfdc2e76a0ef5d50926307b6d62ebbd8237fb229251f7a31c59e780cc06
b7f200dafd586786fb9d1170529e9d231fe92abfe8ad055d70eb36c2aa829d3fdc5b8abb2bd5758a6b675176280d310
0999197912f9c43ca5f32e5031b14160a44c921f9545cddb47fab8d98926d609776b

Висновок

В процесі виконання цієї лабораторної роботи ми вдосконалили свої навички роботи в команді, а також дуже довго шукали помилки через які сталося проблема з розшифруванням, проте розібратися не вдалося