Київський національний університет імені Тараса Шевченка
Факультет комп’ютерних наук та кібернетики
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації

Лабораторна робота №6
“Шифрування і дешифрування тексту за допомогою алгоритму RSA”

Виконали студенти 3-го курсу
Групи ІПС-32

Роботу виконали:
Група 1:
Ольховатий Ігор
Ковальов Володимир
Тряско Софія
Група 2:
Цілинко Олександр
Бондар Юлія
Волик Артем

Київ 2023

Завдання:

Поділитись на 2 групи, кожна придумує довільне повідомлення і шифрує його за допомогою алгоритму RSA. Потім обмінятись цими повідомленнями і розшифрувати їх.

Розв'язання

Процес шифрування групи 1:

Маємо повідомлення

"Футбол - це не просто спорт, це справжнє мистецтво командної гри, що завжди залишає за собою найяскравіші спогади та емоції."

Закодуємо його за допомогую алгоритма RSA

Публічний ключ наступний: {(13132626114134605883, 14136956405830185797)}

Приватний ключ: {(1200490441813743239, 14136956405830185797)}

Кодуємо його наступним чином:

- Перетворюємо символи на їх чисельні значення в ASCII таблиці
- Кодуємо відповідні числа за допогою публічного ключа

Наприклад:

Ф $-$ 1060, тоді $c = E(m) = m^e \, (mod\, n) = 1060^{13132626114134605883} \, (mod$ $14136956405830185797) = 11405649372582354774$

Тоді маємо наступний шифро-текст:

11405649372582354774, 12990052678051057735, 4203146589378850902, 1580202565455666549, 3983263123331534860, 6829662739827557311, 3699822737583698530, 11060948036205744358, 3699822737583698530, 13042046993400951095, 7165535184287608234, 3699822737583698530, 10050645133951669122, 7165535184287608234, 3699822737583698530, 12068281334691958267, 65064872627614085 40, 3983263123331534860, 44309761273407828 04, 4203146589378850902, 3983263123331534860, 3699822737583698530, 4430976127340782804, 12068281334691958267, 3983263123331534860, 65064872627614085 40, 4203146589378850902, 12663205136557715356, 3699822737583698530, 13042046993400951095, 7165535184287608234, 3699822737583698530, 4430976127340782804, 12068281334691958267, 65064872627614085 40, 78779193720081475 40, 11513209865318520218, 767857583671038635, 10050645133951669122, 11501451043561312565, 3699822737583698530, 11834742527589925315, 7733342600719615744, 4430976127340782804, 4203146589378850902, 7165535184287608234, 13042046993400951095, 4203146589378850902,

1151320986531852021 8, 3983263123331534860, 3699822737583698530, 10944989869356555711, 3983263123331534860, 11834742527589925315, 7877919372008147540, 10050645133951669122, 13243105840508971097, 10050645133951669122, 3983263123331534860, 13240662620332118693, 3699822737583698530, 7066910154934849642, 6506487262761408540, 7733342600719615744, 12663205136557715356, 3699822737583698530, 7428482245009646229, 3983263123331534860, 3699822737583698530, 4287732866816756017, 7877919372008147540, 1151320986531852021 8, 767857583671038635, 13243105840508971097, 7733342600719615744, 3699822737583698530, 4287732866816756017, 7877919372008147540, 6829662739827557311, 7733342600719615744, 13687389357821367166, 7877919372008147540, 11501451043561312565, 3699822737583698530, 4287732866816756017, 7877919372008147540, 3699822737583698530, 4430976127340782804, 3983263123331534860, 1580202565455666549, 3983263123331534860, 10684648252330451463, 3699822737583698530, 10050645133951669122, 7877919372008147540, 38428500656876418 46, 8621982684730301877, 4430976127340782804, 10944989869356555711, 6506487262761408540, 7877919372008147540, 1151320986531852021 8, 8440101988021434057, 13687389357821367166, 8440101988021434057, 3699822737583698530, 4430976127340782804, 12068281334691958267, 3983263123331534860, 7066910154934849642, 7877919372008147540, 13243105840508971097, 7733342600719615744, 3699822737583698530, 4203146589378850902, 7877919372008147540, 3699822737583698530, 7165535184287608234, 11834742527589925315, 3983263123331534860, 13042046993400951095, 8440101988021434057, 13240662620332118693, 13060623554361294918

Процес дешифрування групи 2

Цей текст зашифрованний за допомогою алгоритму RSA. Спробуємо його дешифрувати

Беремо закритий ключ для дешифрування:{(1200490441813743239, 14136956405830185797)}

$m = 11405649372582354774^{1200490441813743239} (mod\ 14136956405830185797) = 1060$, що відповідає букві Ф в таблиці ASCII

Так робимо далі за допомогою програми написаної на мові Python

Отримаємо наступний набір чисел
1060, 1091, 1090, 1073, 1086, 1083, 32, 45, 32, 1094, 1077, 32, 1085, 1077, 32, 1087, 1088, 1086, 1089, 1090, 1086, 32, 1089, 1087, 1086, 1088, 1090, 44, 32, 1094, 1077, 32, 1089, 1087, 1088, 1072, 1074, 1078, 1085, 1108, 32, 1084, 1080, 1089, 1090, 1077, 1094, 1090, 1074, 1086, 32, 1082, 1086, 1084, 1072, 1085, 1076, 1085, 1086, 1111, 32, 1075, 1088, 1080, 44, 32, 1097, 1086, 32, 1079, 1072, 1074, 1078, 1076, 1080, 32, 1079, 1072, 1083, 1080, 1096, 1072, 1108, 32, 1079, 1072, 32, 1089, 1086, 1073, 1086, 1102, 32, 1085, 1072, 1081, 1103, 1089, 1082, 1088, 1072, 1074, 1110, 1096, 1110, 32, 1089, 1087, 1086, 1075, 1072, 1076, 1080, 32, 1090, 1072, 32, 1077, 1084, 1086, 1094, 1110, 1111, 46

Логічно уявити, що ці числа відповідають номер літер в таблиці ASCII
Використовуючи, цей факт отримаємо наступний дешифрований текст
“Футбол - це не просто спорт, це справжнє мистецтво командної гри, що завжди залишає за собою найяскравіші спогади та емоції.”

Процес шифрування групи 2:
Шифруємо наступне повідомлення
“*Сьогодні ввечері очікується ясне небо та тепла температура повітря. Температура становитиме близько +25°C, тож це чудова погода для прогулянки.*”

За допомогою відкритого ключа

public key: {(1609757921455110451, 6813457573232032367)}

private key: {(6600090227272859947, 6813457573232032367)}
За тим самим алгоритмом описанним у попередній частині
Отримаємо шифро-текст:
[2422865634051323636, 6324472272912065146, 3090057826641142596, 1847374795490363788, 3090057826641142596, 6560881386565811019, 333609281737137923, 4793102118394883365, 5088069616292577071, 3993451918043128209, 3993451918043128209, 3867616935704300217, 6337257959043829914, 3867616935704300217, 5259423805083950261,

4793102118394883365, 5088069616292577071, 3090057826641142596, 6337257959043829914, 4793102118394883365, 145535019619580292, 1690886867555980701, 3603536249652260563, 1020109975686175065, 6324472272912065146, 3332528915366586089, 652486738847056129, 5088069616292577071, 652486738847056129, 3332528915366586089, 333609281737137923, 3867616935704300217, 5088069616292577071, 333609281737137923, 3867616935704300217, 5837492750129277879, 3090057826641142596, 5088069616292577071, 1020109975686175065, 5957658370209471084, 5088069616292577071, 1020109975686175065, 3867616935704300217, 2114729664562384756, 6691563218889447758, 5957658370209471084, 5088069616292577071, 1020109975686175065, 3867616935704300217, 3719756223500037235, 2114729664562384756, 3867616935704300217, 5259423805083950261, 5957658370209471084, 1020109975686175065, 1690886867555980701, 5259423805083950261, 5957658370209471084, 5088069616292577071, 2114729664562384756, 3090057826641142596, 3993451918043128209, 4793102118394883365, 1020109975686175065, 5259423805083950261, 652486738847056129, 6027648344304130707, 5088069616292577071, 801937565859161170, 3867616935704300217, 3719756223500037235, 2114729664562384756, 3867616935704300217, 5259423805083950261, 5957658370209471084, 1020109975686175065, 1690886867555980701, 5259423805083950261, 5957658370209471084, 5088069616292577071, 3332528915366586089, 1020109975686175065, 5957658370209471084, 333609281737137923, 3090057826641142596, 3993451918043128209, 1614972799972378613, 1020109975686175065, 1614972799972378613, 3719756223500037235, 3867616935704300217, 5088069616292577071, 5837492750129277879, 6691563218889447758, 1614972799972378613, 3031110212899310114, 6324472272912065146, 145535019619580292, 3090057826641142596, 5088069616292577071, 666855754385039480, 2999679471975062122, 4852317854835055524, 5087104348629221509, 4159835436496262533, 4399874707315412277, 5088069616292577071, 1020109975686175065, 3090057826641142596, 5888961315038043231, 5088069616292577071, 341425233423705019, 3867616935704300217, 5088069616292577071, 6337257959043829914, 1690886867555980701, 6560881386565811019, 3090057826641142596, 3993451918043128209, 5957658370209471084,

5088069616292577071, 2114729664562384756, 3090057826641142596, 1847374795490363788, 3090057826641142596, 6560881386565811019, 5957658370209471084, 5088069616292577071, 6560881386565811019, 6691563218889447758, 652486738847056129, 5088069616292577071, 2114729664562384756, 5259423805083950261, 3090057826641142596, 1847374795490363788, 1690886867555980701, 6691563218889447758, 652486738847056129, 333609281737137923, 145535019619580292, 1614972799972378613, 60276483443041307077]

Процес дешифрування групи 1

Для кожного з чисел, що записані у зашифрованій послідовності використовуємо формулу:

$$m = a_i^d (mod\ n), \quad private\ key = (d,\ n)$$

Тобто:

$$2422865634051323636^{66000902272728599947}\ (mod\ 68134575732320323677) = 1057$$

І так далі

У результаті має наступну послідовність чисел, що репрезунтують номери символів у ASCII таблиці:

1057 1100 1086 1075 1086 1076 1085 1110 32 1074 1074 1077 1095 1077 1088 1110 32 1086 1095 1110 1082 1091 1108 1090 1100 1089 1103 32 1103 1089 1085 1077 32 1085 1077 1073 1086 32 1090 1072 32 1090 1077 1087 1083 1072 32 1090 1077 1084 1087 1077 1088 1072 1090 1091 1088 1072 32 1087 1086 1074 1110 1090 1088 1103 46 32 1058 1077 1084 1087 1077 1088 1072 1090 1091 1088 1072 32 1089 1090 1072 1085 1086 1074 1080 1090 1080 1084 1077 32 1073 1083 1080 1079 1100 1082 1086 32 43 50 53 176 67 44 32 1090 1086 1078 32 1094 1077 32 1095 1091 1076 1086 1074 1072 32 1087 1086 1075 1086 1076 1072 32 1076 1083 1103 32 1087 1088 1086 1075 1091 1083 1103 1085 1082 1080 46

Тоді отримане розшифроване повідомлення має наступний вигляд:

Сьогодні ввечері очікується ясне небо та тепла температура повітря. Температура становитиме близько +25°C, тож це чудова погода для прогулянки.

Література:

- Лекції з предмету “Математичні основи захисту інформації”
- https://dou.ua/forums/topic/43026/
- https://www.techtarget.com/searchsecurity/definition/RSA