

МІНІСТЕРСТВО ОСВІТИ, НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ» ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

АСИМЕТРИЧНІ КРИПТОСИСТЕМИ ТА ПРОТОКОЛИ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Підготували:

студенти 4 курсу

групи ФІ-84

Ковальчук О.М.

Коломієць А.Ю.

Криптосистема Рабіна

Атака на протокол доведення знання без розголошення

Мета лабораторної роботи

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

Комп'ютерний практикум включає в себе два завдання: реалізацію розширеної криптосистеми Рабіна та реалізацію атаки на описаний протокол доведення із нульовим розголошенням.

Реалізація криптосистеми Рабіна виконується таким саме чином, як і реалізації криптосистеми **RSA** у *комп'ютерному практикумі №*2. Основні операції (генерування ключів, шифрування/розшифрування, постановка/перевірка підпису) необхідно оформлювати високорівневими процедурами **GenerateKeyPair()**, **Encrypt()**, **Decrypt()**, **Sign()**, **Verify()**.

Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою:

https://asym-crypt-study.herokuapp.com/?section=rabin

Наприклад, для перевірки коректності операції шифрування необхідно:

- а) зашифрувати власною реалізацією повідомлення для серверу та розшифрувати його на сервері;
- б) зашифрувати на сервері повідомлення для вашої реалізації та розшифрувати його локально.

Для проведення атаки на протокол доведення із нульовим розголошенням також необхідно користуватись тестовим середовищем.

За адресою:

http://asymcryptwebservice.appspot.com/?section=znp

проживає сервер, який генерує ключі **RSA** довжиною **2048 біт** та користується описаним протоколом, щоб довести будь-кому своє знання розкладу модуля на прості множники.

Кроки взаємоді з сайтом під час проведення атаки:

Rabin Testing Environment

- 1. Реалізуйте допоміжне програмне забезпечення для проведення сценарію атаки.
- 2. Згенеруйте на сервері ключі для аналізу. Сервер поверне вам значення модуля п (це значення буде існувати доти, доки ви не завершите сесію зв'язку).
- 3. Користуючись формою введення, надсилайте серверу випадкові t, поки атака не завершиться успіхом. Зафіксуйте, з якої спроби вам вдалось зламати ключ.
- 4. Продемонструйте викладачеві вашу перемогу над бездушною машинерією.

Хід роботи

Опис труднощів, що виникали, та шляхів їх розв'язання

Під час виконання лабораторної роботи, були труднощі в реалізації форматування повідомення, не досить зрозуміло, як форматується і розформатовується повідомлення. Вирішенням цього було накладання маски, та зняття з повідомлення. Також були помилки при написанні коду в алгоритмі розшифрування, що пов'язано з обчисленням символа Якобі, для цього тестувалася функція на тридцять значень згенеровані довільним чином, та знаходилися місця в коді де символ Якобі обчислювався не досить коректно. Помилки котрі були в методичних рекомендаціях відшукувалися в іноземних джерелах.

Значення модуля п, згенероване сервером

Server Key Encryption Decryption Signature Verification Colear Key size Signature Modulus S520944EAB0085197FDA61DD2C31C2CB48A2066ED4D8119F76F0BA6022B59626A57714E71C198C16E2CA B 1A2C6AE536255B38B1D2B418B87D92EE6D0FDD0FB1DC02A78648F81773AA01A85CD66EAF1F594585D168

Чисельні значення прикладів відкритого тексту, шифротексту, цифрового підпису у схемі Рабіна для A і B

Шифрування

- input other for encryption:

-moduls:

85920944EAB0065197FDA61DD2C31C2CB48A2066ED4D8119F76F0BA6022B59626A57714E71C198C16E2CACB902 776DE285BF613B9C0C4F4740AD10F3C8AC9B41

-constant:

1A2C6AE536255B38B1D2B418B87D92EE6D0FDD0FB1DC02A78648F81773AA01A85CD66EAF1F594585D1684F7F2F EB384BEB2825F566A1BBDCBBC4A7EB86992631

-message:

- encryption message:
 - ciphertext:

5A36D5DDBB14A6D4DF4502362DB8E2E4E69552DA6028BB1AE5DB768415794E8B031BCA351FA01F6D6FE574596FC2ECC8B78A7028EF3F50508F4F6CB3AA6ACA7E

- parity:

1

- jacoby symbol:

1

Взаємодія із сайтом

Server Key Encryption	Decryption				
Decryption	• Clear				
Signature	Ciphertext	5A36D5DDBB14A6D4DF4502362DB8E2E4E69552DA6028BB1AE5DB768415794		Bytes	
Verification	Parity	1	Jacobi Symbol	1	
		Decrypt			
	Message	047242424266253459824	457924562452645621641261852463423654	1813542945238461	184527642342

Розшифрування

- input other for decryption:
 - public constant: 3426599029FDA5D8ECD7ADCC7146805D0F19A5B9BCFDB
 - public moduls:

A5182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D348831BC3A891B27E696C394DE92FF4A66CB55FE16C81779

- ciphertext:

131A23087F8AE6BF10621449DEFAB259AA56BF5E6463D78A3896E3178AD06EB661389A891EC4ACD24BA95862C9 CB0F948995EA2419CEBF1659E4572D5D712219

- parity:

0

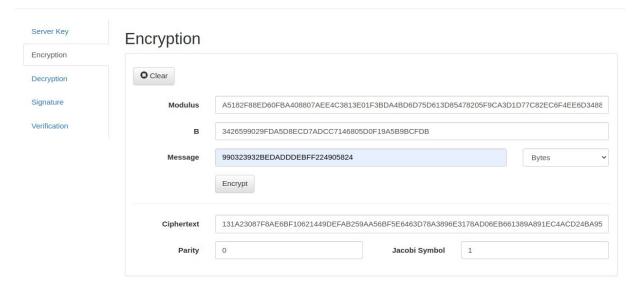
- jacoby symbol:

1

- decryption cryptogram:

990323932BEDADDDEBFF224905824

Взаємодія із сайтом



Цифровий підпис

- -input other for digital signature:
 - public constant:

3426599029FDA5D8ECD7ADCC7146805D0F19A5B9BCFDB

- public moduls:

A5.182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D348831BC3A891B27E696C394DE92FF4A66CB55FE16C81779

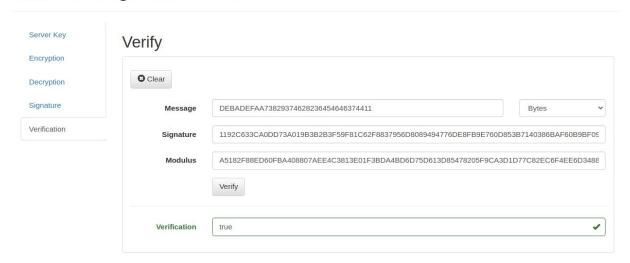
-message:

DEBADEFAA73829374628236454646374411

- digital signature:

 $\tt 1192C633CA0DD73A019B3B2B3F59F81C62F8837956D8089494776DE8FB9E760D853B7140386BAF60B9BF09BD890F68EF9DEADCC3163955B5A733E20F5AAEC02F$

Взаємодія із сайтом



Перевірка цифрового підпису

- -input other for verification:
 - -moduls

85920944EAB0065197FDA61DD2C31C2CB48A2066ED4D8119F76F0BA6022B59626A57714E71C198C16E2CACB902 776DE285BF613B9C0C4F4740AD10F3C8AC9B41

-message:

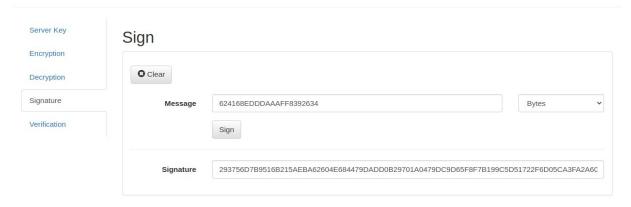
624168EDDDAAAFF8392634

-signature:

293⁷56D7B9516B215AEBA62604E684479DADD0B29701A0479DC9D65F8F7B199C5D51722F6D05CA3FA2A607A03E 427FBFA83ADF320050478E4C1975435ED4C4A7

- verification:
 - -digital signature pass examination: 624168EDDDAAAFF8392634

Взаємодія із сайтом



Zero knowledge protocol

-zero knowledge protocol:

- input moduls:

ABDABD1183B31FC6EA4D3A1F32231DEC2E1A9FD46F4A279C56364439DD13D29CC9112D907E62FBBABAE23C9A6EF48BF18 6573ACA9609391A44B2D5D5BBF6A45DC7E5FBEC33B83FB90FAE8846D3DECF035E4E804C8A9CB3350BC19BD3518A319C79 02C2F64D6FFA8AD3D3031B8E8C6B042968BD1F9555A8670B2582134E0388B8D0A3F072252F1F9563B05E6FC7EFFE01346 52992C04F99E35FE309409300533D6C1D0253921B6D361B4B6CEA595EACCB766F3699A44A56FDF5B072280EDB4DEBB1D5 D6EDB36CC9EA38A0CEBA7736577A5F32BC2C20474176AC637175D45EFC379CACEB99F583FBE2F19E5A2E653BD2AF2F7FB E980BDDB76FC4D34B4905FC39F5

- send number:

78AADF66A5986E1BBE2F1CA9427553B93293411F58C9AB6F36D262C87CEA4FAA59373FE916291EC0718E86C063147B538 ECE15AFE55FEFE139BC073769943061A5EBA151AF98C5902C933A17CF21A30CE0860F091736DFE89D835C167E4D6E1432 510A1D12C1B168C8B1C079C24F4DDEB96DFD9CB4DCA758B4343E1A25100

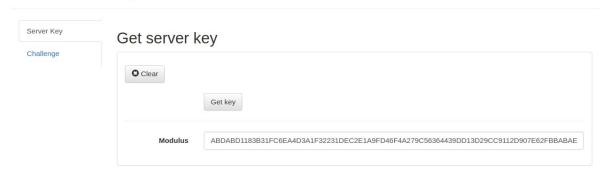
- root number:

 $28F082FB86ADD038BB13C88E6CE8286081051B719B701599EDDAD0057D72A76AAD45C1A62D2EA65D1D0425A1B8A5D2AFB\\6EF6D2A58E676101F65846D8809090$

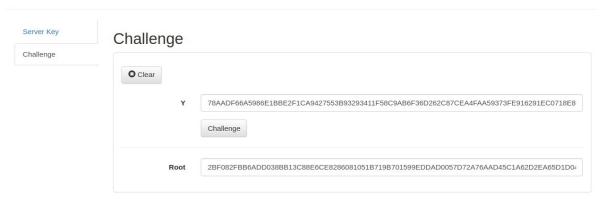
Good proof.

Відомості з сайту

Zero Knowledge Protocol



Zero Knowledge Protocol



Покрокову реалізацію сценарію атаки на протокол, із зазначенням усіх проміжних значень

(для спрощення значення генеруються локально в нашій програмі)

- -attack on crypto system:
- public key Client:
 - public constant:

3426599029FDA5D8ECD7ADCC7146805D0F19A5B9BCFDB

- public moduls:

A5182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D348831BC3A891B27E696C394DE92FF4A66CB55FE16C81779

- public key Server:
 - public constant:

D3B3C29D3CC8ED7E01E4A3305BB5C81C3587C641781BB1

- public moduls:

 $4 \bar{b}. 7663D049D35D6738D88084B6092420DDFDF73A7AA6FD7EDBFF9927BFD778FB7813A41A954B154C00FDE2432B23737CE161AAE1FE06B2745DD865125E6F7F35$

- input moduls for attack:

4B7663D049D35D6738D88084B6092420DDFDF73A7AA6FD7EDBFF9927BFD778FB7813A41A954B154C00FDE2432B23737CE 161AAE1FE06B2745DD865125E6F7F35

- attack get key:

7E776A493C52657245E6221C0DF641C8DD3C7FEE96D84EE1C25760811DD22C2F

- number of iteration for cracking system:

2

Перевірка, що ви дійсно знайшли розклад п на прості множники

- compare with secrete parametre Server:
 - public constant:

D3B3C29D3CC8ED7E01E4A3305BB5C81C3587C641781BB1

- secrete p:

7E776A493C52657245E6221C0DF641C8DD3C7FEE96D84EE1C25760811DD22C2F

- secrete q:

98C14A3F119534B09C6B04FCBC7DADC7F9D4A4607720834196988101250BBDDB

Приклад генерування випадкових простих чисел Блюма

-generation bloom prime number fixes size:

-generation bloom prime number fixes size:

- public moduls:

A5182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D348831BC3 A891B27E696C394DE92FF4A66CB55FE16C81779

Висновки

Під час виконання комп'ютерного практикуму ми навчилися реалізовувати розширену модель, криптосистеми Рабіна та використовувати апарат абстрактної алгебри та теорії чисел на практиці. Багато алгоритмів було тяжко реалізовувати через абстрактність їх опису.

Посилання на програмну реалізацію:

https://gitlab.com/andrew.kolomiets/asymmetric-cryptography-3.git