Механика Транспорт Комуникации

Научно списание http://www.mtc-aj.com

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 13, брой 1, 2015 г.
статия № 1105

ПРОЕКТИРАНЕ И ИЗСЛЕДВАНЕ НА ХИБРИДНА КРИПТОГРАФСКА СИСТЕМА ОСИГУРЯВАЩА ЗАДАДЕНО НИВО НА СИГУРНОСТ ПРИ ПРЕДАВАНЕ НА ИНФОРМАЦИЯ

Мария Ненова
mvn@tu-sofia.bg

Технически Университет – София, бул. „Кл. Охридски”, БЪЛГАРИЯ

Ключови думи:*криптиране, асимиетрични алгортми за криптиране, симетрични алгоритми за криптиране, хеш функции, RSA, AES*

Резюме: *Представена е практическа реализация на криптиране чрез прилагането на RSA асиметричен алгоритъм, реализация на хибриден (комбинация между симетричен и асиметричен) алгоритъм, използван за защита на информацията, както и изследване на времето необходимо за процеса на криптиране при различни размери на използваните ключове.*

1. УВОД

Алгоритъмът разработен от Рон Ривест, Ади Шамир и Лен Аделман (RSA) през 1977. Той е най-често използваният и доказал устойчивостта си асиметричен криптографски алгоритъм. Алгоритъмът RSA се основава на математическата особеност, че е лесно да се намерят и умножат големи прости числа, но е изключително трудно да се получат по обратния път от тяхното произведение [1]. В RSA се използва понятието частен и публичен ключ, представени с прости числа с много голям (със 100 или повече цифри) размер. В настоящия доклад е разгледантози алгоритъм в комбинация със симетричен [2], [3].

При всяка една схема за криптиране има два важни фактора, а именно: типът алгоритъм, който ще бъде използван и режима, в който ще работи [2]. Тук са анализирани и изследвани Advamced Encription Standard (AES) – 256алгоритъм и RSA. [4], [5].

2. КРИПТИРАЩ АЛГОРИТЪМ RSA

С цел реализацията на RSA алгоритъмае необходимо да се генерират двойка ключове (секретен и публичен). Понякога реализацията може да се базира и на използването само на един ключ (публичен) [6], [7], [8]. При първия вариант се генерират две прости числа, които представляват основата за изчислението на публичния и секретния ключ. При втория вариант се въвежда директно RSA модула ***n*** и публичния ключ. Избират се две прости числа ***p***и ***q*****,** използвани за генериране на ключове. След това се извеждат параметрите необходими за генериране на двойката ключове (секретен и публичен).

2.1 Параметрите, които подлежат на избор са:

- методът, по който да се реализира генерирането на числата;
- опцията дали двете числа (***p*** и ***q***) са в еднакъв диапазон или да има възможност за изборв различен;
- границите, в които да бъдат генерирани.

За първия параметър е избран метода с Тест на Ферма (Fermat Test), а за втория е избрангранициите да са независими една от друга.

При третият параметър се избрат две случайни прости числа *p* и *q*, в рамките на 215 – 256 бита. Колкотоса по-големи числата,които се генерират, толкова по защитени саданните, които ще бъдат защитавани в последствие. От големината на двете прости числа *p* и *q* зависи и до колко символа може да се криптират в един блок след това.

Фиг. 1: Генериране на прости числа

След като вече са генерирани простите числа се преминава към изчисляването на другите параметри на RSA алгоритъма. Първият, от които е модулът*N*, следващият е *phi(N) = (p-1)(q-1)*, а последните два са публичния и секретния ключ.

Анализът, който се провежда може да бъде върху данни с различен формат - ASCII или определена азбука. Избрано е представяне в ASCII код. Режимът на работа е нормалния за RSA вариант и метод за представяне на текста в числа b-adic. След това е дефинирана максималната дължина на блоковете.

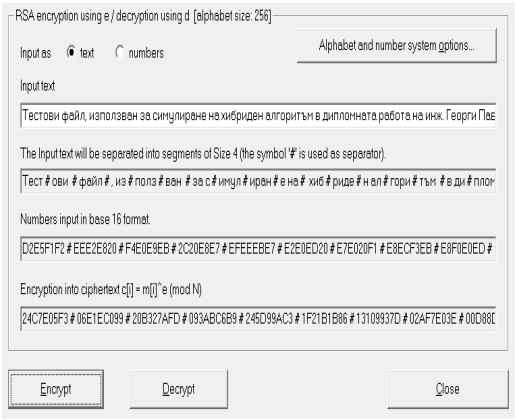
Накрая с цел онагледяване е показано криптираното съобщение, шестнадесетичен вид.

2.2 Процедурата по криптиране преминава през следните стъпки:

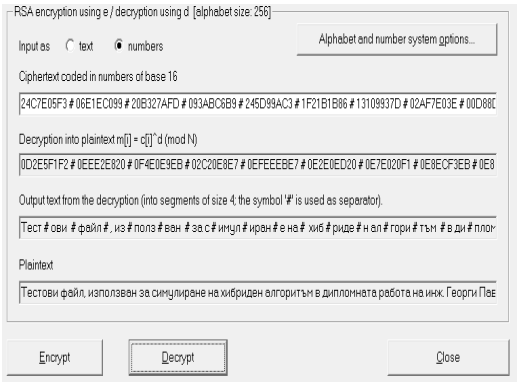
1) Избраният текст се разделя на блокове с предварително избрана дължина. Блоковете са разделени един от друг чрез специалния символ #;
2) Текстът, разделен на блокове, се конвертира в числа в шестнайсетичен формат чрез метода *b-adic*, който бе избран на предходния етап;
3) Резултатът накрая е получаването на криптирани данни.

Процедурата по декриптиране е аналогична и протича по обратния ред на процедурата по криптиране. При декриптирането вместо съобщение в явен вид, се въвеждат криптираните данни и при правилното спазване на алгоритъма се получава изходното съобщение. Ако то съвпада с първоначалното, то тогава може да се направи извода, че интегритета и автентификацията на данните са запазени.

На следващите две фигури (фигура 2 и 3) са представени съответно процедурите по криптиране и декриптиране на данните, чрез използването на RSA алгоритъма.



Фиг. 2: Криптиране на съобщението



Фиг. 3: Декриптиране на съобщението

3. СИМУЛАЦИЯ НА ЦЯЛОСТНА КРИПТОГРАФСКА СИСТЕМА, ИЗПОЛЗВАЩА ХИБРИДЕН АЛГОРИТЪМ ЗА КРИПТИРАНЕ

В тази точка е представена симулацията на метода за защита на данните чрез криптиране, базирано на комбинацията между симетрични и асиметрични алгоритми за криптиране. Разгледаният метод за защита се състои в използването на хибриден криптографски подход, чрез съчетаването наAdvamced Encription Standard (AES) – 256bit алгоритъма с RSA. За допълнителна защита и гарантиране на автентификацията се използва сравнение на хеш стойности, изчислени чрез използването на еднопосочната хеш функция SHA 1– 256, както от изпращащия съобщението, така и в приемната страна.

3.1 ОСНОВНИТЕ СТЪПКИ ПРИ РЕАЛИЗАЦИЯТА СА:

1. Избира се входен файл и парола. В случая е избран текстовият файл с дефинирано от изпращащата страна име. За парола е използвано името на „*Технически Университет - София“*.

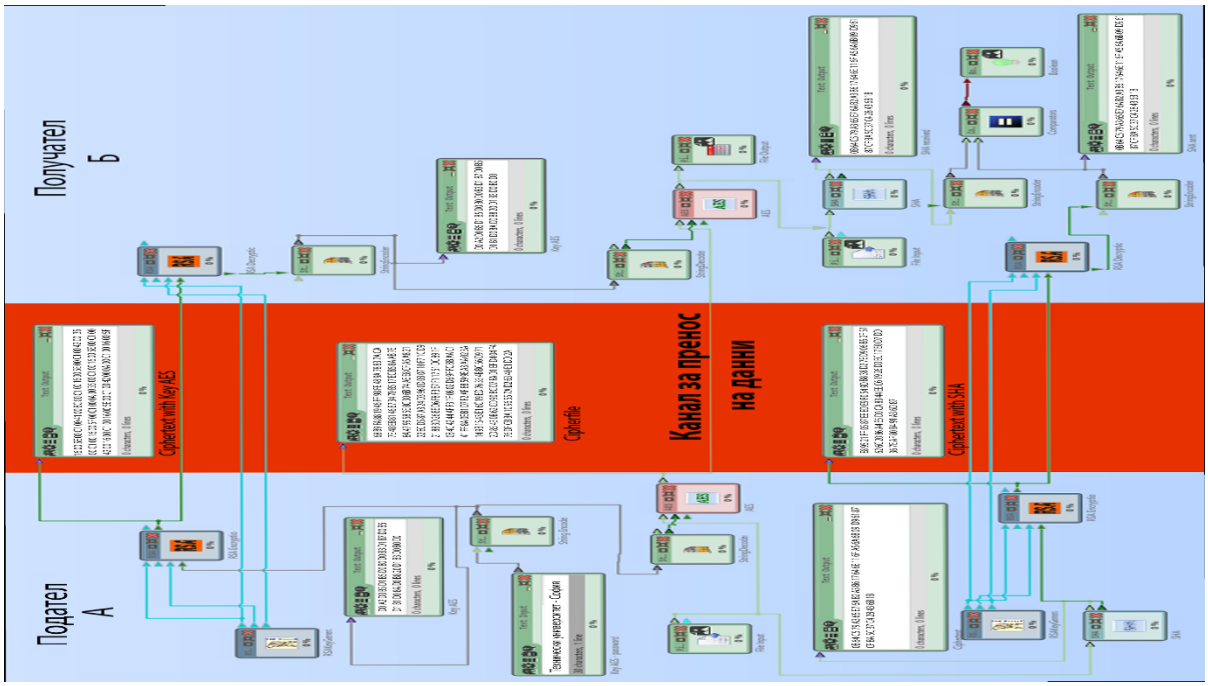
2. Следващата стъпка е да се защити избраната парола, която се явява ключ K_{AES} на AES – 256 алгоритъма, като той в последствие е защитен чрез криптиране с публичния ключ на получателя. Този защитен вече ключ може да бъде видян само от получателя на съобщението. Той използвайки секретния си ключ ще получи чрез асиметричния RSA алгоритъм в явен вид за да може да го използва при декриптирането на съобщението. Изчислява се хеш стойността на избрания файл чрез използване на хеш функцията SHA 1– 256.

3. Изчислената хеш стойност се криптира чрез асиметричния RSA алгоритъм, и получената криптирана хеш стойност, заедно с криптирана парола и криптираните данни се изпращат по открит комуникационен канал за пренос на данни.

4. Отсрещната страна получава криптирания файл и криптирана парола. След което декриптира криптираната парола чрез RSA алгоритъма, и получава явната парола. Криптираният файл се декриптира чрез получената явна парола и AES алгоритъма. Файлът вече е в явен вид и може да бъде записан.

5. Изчислява се хеш стойността на получения файл чрез използване на хеш функцията SHA 1 – 256 и се сравнява с получената от изпращащия съобщението хеш стойност.

На следващата Фигура4е представена демонстрация на пълната криптографска система, базирана на използването на разгледания хибриден криптографски алгоритъм.

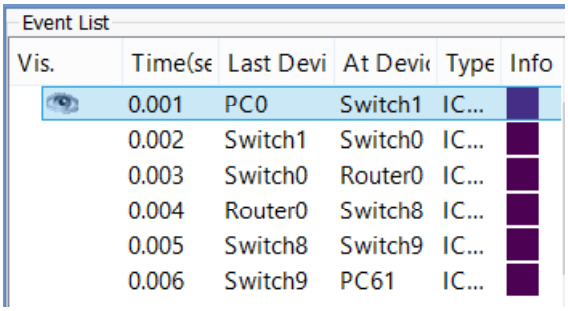


Фиг. 4: Структура на цялостната криптосистема

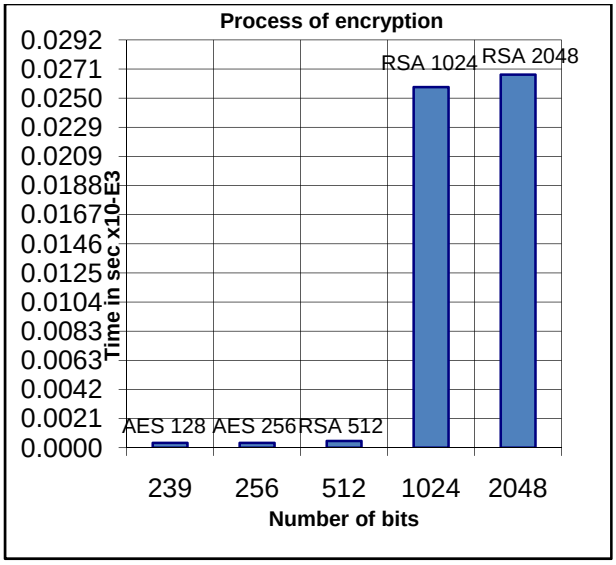
4. ПРОВЕРКА НА ПОВЕДЕНИЕТО НА ПАКЕТИ В МРЕЖАТА

Както вече беше разгледано е необходимо специалистите по сигурността, отговарящи за сигурния пренос на данни, да съберат възможно най-много информация за мрежата, която е обект на защита, спецификата й, анализ на трафика и др.Характерна особеност, е, че опитът за анализ и проследяване на събитията в мрежата, не влияе на потребителите.

Тук е представено симулирано предаване на пакети между произволно избрани комуникационни устройства в мрежата за пренос на данни. В конкретния случай, двете устройства са съответно, компютърът PC0, който се явява източник на пакетите и компютърът PC61, който се явява крайна дестинация на пакетите. На фигура 5е представен пълният списък на устройствата, участващи в обмена на пакети между PC0 и PC61. Освен това в колонката Time (sec) е представено времето за предаването на един пакет от едно устройство до друго.



Фиг. 5: Пълният маршрут на пакетите обменяни между компютри PC0 и PC61



Фиг. 6: Пълният маршрут на пакетите обменяни между компютри PC0 и PC61

От резултатите получени на графиката се вижда, какво време отнема процеса на криптиране на изходния явен текст, ако се приложат AES алгоритъм от 128 до 512 бита размер на ключа, RSA от 512 до 2048 бита, както и комбинация от двата.

5. ЗАКЛЮЧЕНИЕ

Проведеният в доклада анализ е въз основа на използването на хибриден криптиращ алгоритъм. Този алгоритъм съчетава характеристиките на симетричните и асиметричните криптографски алгоритми, като взима бързината на симетричните и сигурността на асиметричните. Като допълнителна защита е реализирано сравнение на входния с изходния файл, чрез изчисляването на уникални хеш стойности с помощта на SHA 1– 256 функцията, която се счита за по-надеждна от широко използваните MD4 и MD5 (които са вече компрометирани).

Асиметричният криптиращ алгоритъм, който е използван е RSA, намиращ широко приложение в цифровите подписи, в банките, в SSL сертификатите и др. Симетричният криптиращ алгоритъм, който е използван е AES – 256, (Rijndael), който се използва в различни организации и устройства по целия свят (въпреки, че в момента тече конкурс за нов алгоритъм, който да стои зад AES стандарта).

Сигурността на използвания криптографски метод се определя чрез неговата устойчивост на атака с пълно изброяване (комбиниране, brute-force attack) на възможните стойности. В конкретния случай необходимите опити за разбиването на ключ с дължина 256 бита са $1{,}16*10^{77}$, което е изключително голям брой комбинации.

От казаното до тук се вижда, че всички използвани алгоритми са с дължина на ключа до 512 бита, тъй като така се избягва контрола върху тях от страна на държавата.

ЛИТЕРАТУРА:

[1] Adi Shamir, RivestR., Adleman L.,A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLICKEY CRYPTOSYSTEMS.*Communications of the ACM*, 21:120–126, 1978.
[2] William Stallings. CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICES. Prentice Hall, November 16, 2005.
[3] B. H. Thomas: AN INVITATION TO CRYPTOLOGY, ISBN-13: 978-0130889768, Aug 2001.
[4] Elaine Barker and Allen Roginsky, NIST SPECIAL PUBLICATION 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, 2011.
[5]Bertoni, G., Breveglieri, L., Koren, I., Maistri, P., ERROR ANALYSIS AND DETECTION PROCEDURES FOR A HARDWARE IMPLEMENTATION OF THE ADVANCED ENCRYPTION STANDARD, IEEE TRANSACTIONS ON COMPUTERS, Vol. 52 , Issue: 4, pp. 492 – 505, April 2003.
[6] Chih-Chung Lu, Shau-Yin Tseng., INTEGRATED DESIGN OF AES (ADVANCED ENCRYPTION STANDARD) ENCRYPTER AND DECRYPTER, The IEEE International Conference on Application-Specific Systems, Architectures and ProcessorsProceedings, pp. 277 – 285, 2002.
[7] Trifonov V, SAFETYAUTOMATA NETWORK FOR INTERLOCKING SYSTEM XXInternational Scientific Conference TRANSPORT 2011, Sofia, Nov 2010 part 3, p.83-88 2011.
[8] Trifonov V, Hristov H., AUTOMATAMODEL FOR SAFETY CRITICAL NETWORK ESI39, European Politechnical University Pernik, 9-10 Jun 2012.

DESIGN AND INVESTIGATION OF A HYBRID CRYPTOSYSTEM PROVIDING DEFINED LEVEL OF SECURITY

Maria Nenova
mvn@tu-sofia.bg

Technical University of Sofia, "St, Kl. Ohridski"blvd., BULGARIA

Key words: *cryptography, symmetric and asymmetric crypto algorithms, hash function, RSA, AES*

Abstract: *In the paper is presented a realization of the cryptography process implementing the RSA asymmetric algorithm together with the AES symmetric algorithm for protection of the transferred data. The time necessary for encryption with different key sizes is investigated.*