A COMPARATIVE ANALYSIS OF DIGITAL SIGNATURE CRYPTOGRAPHIC SYSTEMS

Anastasiya A. Dimitrova

Национален военен университет "В. Левски", Факултет „Артилерия, ПВО и КИС", гр. Шумен, докторант в катедра „Компютърни системи и технологии", anidimitrova3005@abv.bg

Abstract: *The document looks at the technologies and algorithms for encrypting information. There is research of some of the most commonly used digital signature algorithms. A comparative analysis of cryptographic systems for digital electronic signature was performed.*

Keywords: *Digital Signature Algorithm (DSA), Eliptic Curve Cryptography (ECC), Elliptic Curve Discrete Logarithm Problem (ECDLP), Elliptic Curve Digital Signature Algorithm (ECDSA), Rivest, Shamir и Adleman (RSA).*

СРАВНИТЕЛЕН АНАЛИЗ НА КРИПТОГРАФСКИ СИСТЕМИ ЗА ЦИФРОВ ЕЛЕКТРОНЕН ПОДПИС

Анастасия А. Димитрова

I. УВОД

Особена актуалност в последните години придоби проблемът за гарантиране на авторството и сигурността на комуникациите в отворени системи [2, 9, 10]. Значимостта му произлиза от изискванията за получаване на точна и достоверна информация за изпратеното съобщение, неговия подател и получател, при условия на канали за връзка с възможност за подслушване и преднамерени шумове, организирани от престъпни и терористични групировки. При електронната комуникация липсва сигурността на непосредствения контакт с бизнес партньора, като електронните съобщения преминават през много посредници, управляващи своите комуникационни системи по различни комуникационни протоколи, някои от които несигурни. Това изисква повишаване на ефективността на криптографските системи, за да се гарантира, че някой не е прочел или подменил съдържанието на предаваното съобщение.

В наши дни проблемът се решава с използване на механизма на цифровия електронен подпис. По въпроса съществуват множество научни публикации за повишаване на ефективността на асиметричните криптографски системи чрез използването на елиптични криви. Въпреки това, в тази област съществуват голям брой въпроси, които не са изследвани с необходимата изчерпателност. Необходимо е систематизиране на научните методи в областта, които да са оригинални и практически приложими в съвременните комуникационни и информационни системи.

В доклада първо са анализирани основните криптографски примитиви, осигуряващи услугите за информационна сигурност. След това са разгледани асиметричните криптографски системи базирани на елиптични криви, направен е сравнителен анализ на алгоритмите за цифров подпис.

II. ИНФОРМАЦИОННА СИГУРНОСТ

1. Технологии, осигуряващи услугите за информационна сигурност

Основните технологии, осигуряващи услугите за информационна сигурност, са криптиране на данните, хеширане, автентификация и цифров подпис.

Криптиране (шифриране) е математическа процедура за промяна на данните от форма на четливост в друг, неподлежащ на разчитане, вид. Обратното преобразуване на информацията в първоначалния й вид е дешифриране. За целта се използват математически алгоритми, като се цели

да се осъществи безопасно съхранение или предаване на данни по незащитен информационен канал.

Технологиите за криптиране на информация могат да предоставят следните услуги [3]:

- Конфиденциалност, която прави информацията неразбираема за неоторизирани потребители.
- Цялостност на данните, която предоставя доказателство, че информацията не е била променена по неразрешен начин, докато тя се създава, предава или съхранява.
- Автентификация, чрез която се проверява самоличността на потребителя или системата, която създава информацията.
- Оторизация, при която след доказване на самоличността, на обекта се предоставя ключ или парола, която ще му позволи достъп до определени ресурси.
- Недопускане на отхвърляне, което гарантира, че подателят не може да отрече изпращането на съобщението.

2. Основни криптографски примитиви

Симетрични алгоритми за криптиране

Симетричните алгоритми за криптиране (Symmetric Encryption) използват един и същ таен ключ (Secret Key) и криптографски алгоритъм, за да шифрират и дешифрират съобщенията.

При този алгоритъм за шифриране и дешифриране на информацията, подателят и получателят разполагат с един и същи ключ, за използването, на който са се договорили преди началото на комуникацията. Ако ключът не е компрометиран, то при декодирането на шифрованата информация автоматично се извършва идентификация на подателя, тъй като само той, освен получателя, разполага със съответния ключ. Подателят и получателят са единствените физически лица, които имат достъп до секретните ключове и при компрометиране на системата, те са единствените, които носят отговорност. Проблемът, който е актуален и при други криптографски системи, е въпроса свързан с безопасното разпространение на симетричните (секретни) ключове. Алгоритмите за симетрично криптиране използват ключове с малка дължина и позволяват бързото шифроване на относително големи по обем информационни масиви.

В съвременния свят алгоритмите за криптиране се подлагат постоянно на анализ от специалисти от целия свят, за да се утвърдят като „добри" алгоритми. Процесът на криптоанализ се концентрира върху разбиването на ключовете, чрез които е извършено криптирането. Съществува зависимост между алгоритъма за криптиране и дължината на използваните ключове за този алгоритъм, които предлагат определена „сигурност" на криптирането. Тази сигурност се измерва в брой години, които трябва да работят компютърни системи с определена изчислителна мощност, за да разбият ключа. С всеки изминат ден изчислителната мощност на компютрите се увеличава, а паралелните компютърни системи предлагат все повече паралелно работещи процесори, които биха могли да се използват за разбиване на ключовете. Ето защо сигурността на криптиране е относителна и зависи от наличната в момента изчислителна мощност, която може да се използва за разбиване на ключовете.

Асиметрични алгоритми за криптиране

Асиметричните алгоритми за криптиране (Asymmetric Key Algorithms) използва двойка различни ключове за криптиране и декриптиране на текста. Двата ключа са свързани математически. Асиметричното криптиране често се нарича криптиране с публичен ключ (Public Key Encryption). За общуване на две страни са необходими две различни, но свързани стойности за ключовете: публичен и частен.

При този метод на криптиране ключовете за шифриране и дешифриране на информацията са различни, макар и да се генерират на едно и също място. Един от ключовете е общодостъпен (публичен), а другият се съхранява в съответствие с условия, гарантиращи неговата конфиденциалност. Макар и двата ключа да позволяват шифриране и дешифриране на информацията, криптираната с единия от тях може да бъде декриптирана само с другия. Всяка асиметрична криптографска система се явява обект на атака по метода на пробата и грешката, което налага използва-

нето на ключове с по-голяма дължина, от тези в симетричните, при гарантиране на еквивалентно ниво на защита. Това неминуемо довежда до повишаване на изискванията към използвания изчислителен ресурс.

Асиметричните ключове са уязвими за атаки и поради факта, че са по-трудно заменими от симетричните. Ако атакуващият получи достъп до секретен асиметричен ключ, то ще бъде компрометирана не само текущата, но и всички последващи комуникации.

Хеш функции

Хеш функцията (Hash Function) представлява резултатът от еднопосочно математическо изчисление, което приема съобщение с произволна дължина и връща код с фиксирана дължина. Резултатът с фиксирана дължина се нарича хеш (Hash) или отпечатък на оригиналното входно съобщение (Message Digest). Алгоритъмът се нарича „еднопосочен", защото не може да се реверсира резултата, за да се възстанови оригиналното съобщение. За да бъде приложима в криптографията хеш функцията трябва да притежава следните свойства:

- Функцията да бъде постоянна, т.е. един и същи входен аргумент трябва да води до един и същи резултат;
- Функцията трябва да бъде еднопосочна (необратима);
- Резултатът от функцията трябва да бъде случаен, за да се предотврати разбирането на началното съобщение;
- Резултатът от функцията трябва да бъде уникален, т.е трябва да е почти невъзможно да се открият две съобщения, водещи до един и същ представител на съобщение.

Хеш функциите обикновено се използват за проверка на целостта на съобщенията. Промяна само на един символ в оригиналното съобщение, би променила голям брой от битовете в хеш кода [3].

В таблица 1 са представени най-често използваните криптографски алгоритми и предоставените от тях услуги за сигурност.

Таблица 1. *Криптографски алгоритми и предоставените от тях услуги*

Алгоритми	**Крипти-ране**	**Цифров подпис**	**Разпределение на ключове**	**Хеш функция**
Симетрични				
DES, 3DES	✓			
AES	✓			
Blowfish	✓			
IDEA	✓			
RC4	✓			
Асиметрични				
RSA	✓	✓	✓	
ECC	✓	✓	✓	
Diffie-Hellman			✓	
El Gamal	✓	✓	✓	
DSA		✓		
LUC	✓	✓	✓	
Knapsack	✓	✓	✓	
Хеширане				
MD2, MD4 и MD5				✓
SHA				✓
HAVAL				✓

III. АСИМЕТРИЧНИ КРИПТОСИСТЕМИ НА БАЗАТА НА ЕЛИПТИЧНИ КРИВИ

1. Сигурност на криптосистемите базирани на елиптични криви

Всяка криптосистема се основава на трудна математическа задача, която е невъзможно да се реши с наличните технически изчислителни средства. Проблемът с решаването на дискретния

логаритъм е в основата за сигурността на много криптосистеми включително и тези с елиптични криви. Сигурността на ранните криптосистеми с публичен ключ се основава на факта, че е трудно да се разложи на прости множители голямо число, съставено от два или повече големи прости множители. По-специално, сигурността на криптосистемите базирани на елиптични криви се основава на трудността на проблема с дискретния логаритъм при елиптични криви ECDLP (Elliptic Curve Discrete Logarithm Problem). Сложността на решението на дадения проблем се дължи на ресурсно изискващите операции събиране и удвояване на точки. При асиметричните криптосистеми базирани на елиптични криви се приема, че намирането на дискретен логаритъм на случаен елемент от елипсовидна крива по отношение на публично известна базова точка е неосъществимо. Сигурността на криптосистемите с елиптични криви зависи от възможността да се изчисли задачата за умножение на две точки и невъзможността да се изчисли множителя при дадени точки на оригинала и на техния продукт получен при умножението.

Основното предимство, което предоставят асиметричните криптосистеми с елиптични криви, е по-малкия размер на ключа, което от своя страна намалява изискванията към ресурсите за неговото съхранение и предаване. Следователно групата криптосистеми, основани на елиптични криви, може да осигури същото ниво на сигурността, гарантирано от RSA базирана криптографска система, но при по-къс ключ. Например, 256-битов публичен ключ при алгоритъм с елиптична крива гарантира сигурност еднаква с тази на 3072-битов RSA публичен ключ.

Американската агенция за национална сигурност NSA (National Security Agency) през 2010 г. одобри използването на елиптични криви за криптографски цели, като позволява приложението им за защита на информация, класифицирана като строго секретна с 384-битови ключове.

Най-бързият известен алгоритъм за решаване на ECDLP проблема е Ро алгоритъма на Полард. Това е алгоритъм с експоненциално време, което определя по-малките препоръчителни дължини на ключовете при криптосистеми с елиптични криви при осигуряване на еднакво ниво на сигурност. Препоръчваните дължини на ключовете от NIST са представени в таблица 2 [7].

Таблица 2. *Препоръчвани дължини на ключовете от NIST*

Симетрични алгоритми [bits]	**RSA и DH [bits]**	**ECC [bits]**
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Криптосистемите на базата на елиптични криви получават все по-голямо разпространение по-скоро като алтернатива, а не като заместител на RSA системите. Те имат няколко предимства, особено при използването в устройства с ограничени ресурси като маломощни процесори и/или малко памет.

Основните области на приложение на криптосистемите базирани на елиптични криви са:

- мобилна търговия (m-commerce) – WAP, клетъчни телефони, джобни компютри;
- смарт-карти (например Europay, Mastercard и Visa (EMV));
- схеми за генериране на двойка ключове използващи дискретен логаритъм [6]
- споразумение при обмяна на ключове използвани във финансови услуги [5].

В криптосистемите на базата на елиптични криви могат да се идентифицират следните проблеми:

- реалната сигурност на тези системи не е напълно изследвана;
- трудност при генерирането на подходящи криви;
- несъвместимост с другите криптографски системи с открит ключ;
- необходимост от лицензиране и патентоване;
- относително бавни при проверка на електронния цифров подпис [1].

Въпреки тези проблеми криптографията базирана на елиптични криви ECC (Eliptic Curve Cryptography) предоставя математически примитиви с публичен ключ, които използват много по-къси дължини на ключа в сравнение с RSA базираните криптосистеми и тези на алгоритъма на цифров подпис базиран на Gold Diffie-Hellman (DH) алгоритъма. Това е решаващо предимство за вградените устройства, в които мощността, обемът памет и изчислителната мощност обикновено са ограничени. По този начин много приложения преминават към ECC, тъй като изискванията за сигурност се увеличават заедно с ограничаване на използваните ресурси в устройствата [4].

IV. СРАВНЕНИЕ МЕЖДУ АЛГОРИТМИТЕ ЗА ЦИФРОВ ПОДПИС

Сигурността играе важна роля в съвременното виртуално общество. От изключително значение е въпроса да се осигури целостта на предаваните данни, като е важно всички важни данни да бъдат подписани от техния собственик. Цифровият подпис осигурява средство за проверка на целостта на данните, като едновременно с това предоставя сигурност в получателя, че данните са били изпратени от подателя. Основните алгоритми за цифрови подписи, които се използват днес, са алгоритъма на Rivest, Shamir и Adleman (RSA) и Elliptic Curve Digital Signature Algorithm (ECDSA).

1. RSA алгоритъм

Алгоритъмът RSA е разработен в Масачузетския технологичен институт (MIT) през 1977 година от Рон Ривест, Ади Шамир и Леонард Адлеман. Сигурността на RSA алгоритъма се основава на генерирането на големи числа, което означава, че по-дълга битова последователност осигурява по-голяма защита. RSA се използва за криптиране/декриптиране на данни и също има способността да подписва и/или да проверява целостта на пакетите данни. RSA не изисква използването на конкретна хеш функция, така че сигурността на цифровия подпис и криптирането зависи отчасти и от избора на хеш функцията, използвана за изчисляване на подписа.

3. ECDSA

Алгоритъмът за цифров подпис базиран на елиптични криви ECDSA е аналог на алгоритъма за цифров подпис DSA (Digital Signature Algorithm), но е базиран на използването на елиптични криви. ECDSA е разработен през 1985 г. от Нийл Коблиц и Виктор Милър. Схемите ECDSA осигуряват същата функционалност като RSA схемите, включително подпис и/или проверка на подписани пакети. Ограничените по мощност среди, като вградените системи, нямат ресурси да изпълнят 1024-битов RSA алгоритъм, докато позволяват реализирането на 192-битов ECDSA. Размерите на ключовете за ECDSA варира от 163 до 571 бита и 1024 до 15360 бита за алгоритми за RSA [8].

Таблица 2 представя препоръчителните дължини на използваните ключове за RSA и ECDSA алгоритмите в съвременните системи за цифров подпис.

Таблица 3. *Еквивалентни дължини на ключове за RSA и ECDSA*

RSA дължина на ключа (битове)	ECDSA дължина на ключа (бита)
1024	192
2048	256

От таблицата може да се направи изводът, че ECDSA изисква значително по-малък размер на ключовете от RSA за осигуряване на едно и също ниво на сигурност, като предлага по-бързи изчисления и по-малко място за съхранение. Следователно, ECDSA е идеален за ограничени среди, като таблети, смарт телефони, RFID системи и датчици.

V. ЗАКЛЮЧЕНИЕ

RSA и ECDSA са основните алгоритми за цифров подпис доказали своята ефективност срещу съвременните кибератаки, които се характеризират с относително приемлива скорост на криптиране и декриптиране на данните. Алгоритъмът ECDSA поддържа същото ниво на сигурност като RSA алгоритъма при по-малки дължини на използваните ключове и същевременно с това осигурява по-бързи изчисления при по-ниска консумация и по-малък обем памет. В допълнение ECDSA може да генерира ключове с по-висока скорост от RSA при сравними по дължина ключове.

Предимствата на алгоритъма ECDSA спрямо другите криптографски системи за цифров подпис са:

1. Осигурява по-голяма сигурност с по-малки размери на ключовете.
2. Предоставя ефективни и компактни приложения за реализация на криптографски примитиви в чипове с ограничени ресурси.
3. Поради по-малкия размер на чиповете, се намалява количеството отделена топлина и се намалява тяхната консумация.
4. Най-често е подходящ за устройства с малка изчислителна мощност и по-малко памет.
5. Осигурява по-лесни хардуерни реализации.

По-малките размери на ключа при ECDSA алгоритъма позволяват използването на криптографски примитиви осигуряващи конфиденциалност на предаваните данни, проверка на тяхната цялостност и по-бързо генериране на цифрови подписи в ограничени изчислителни устройства, като вградени системи, таблети, смарт телефони, RFID системи, датчици и IoT модули.

References :

1. Ташева Ж. Н. Информационни технологии за сигурност, Издателски комплекс на НВУ „Васил Левски", ISBN 978-954-753-189-5, 2013, 155 с.
2. Ташева Ж. Н., Р. А. Богданов, Анонимна система за комуникации в киберпространството, използваща протокола TOR, Сборник научни трудове от научна конференция 2014 „Защитата на личните данни в контекста на националната сигурност", Факултет „Артилерия, ПВО и КИС", стр. 259-266, ISBN 978-954-9681-49-9.
3. Ташева Ж. Н., Р. А. Богданов, Технологични решения за информационна сигурност, Издателство на НВУ „В. Левски", 2012, 110 с.
4. Verneuil V., Elliptic curve cryptography and security of embedded devices. Diss. Université de Bordeaux, 2012.
5. ANSI X9.63-2011 (R2017) Public Key Cryptography For The Financial Services Industry - Key Agreement And Key Transport Using Elliptic Curve Cryptography. 2017.
6. Barker El., Chen L., Roginsky A., Smid M., NIST Special Publication 800-56A, Revision 2. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, 2018, Avaible from https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-56Ar2.pdf
7. Barker El., NIST Special Publication 800-57 Part 1 Revision 4 Recommendation for Key Management Part 1: General, 2016, Avaible from: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4
8. Levy Sh., Performance and Security of ECDSA, Avaible from https://pdfs.semanticscholar.org/7b20/33159cc8ef7f50619b1592eeea639e2807a3.pdf
9. Nikolov L., Slavyanov Kr., On the contemporary cybersecurity threats, International Scientific Journal Security & Future, Vol. 1 (2017), Issue 3, p. 111-113, ISSN 2535-0668, Avaible from https://stumejournals.com/journals/confsec/2017/3/111

Stoyanova V, Possibilities for the application of social networks in transmission of secret information, International Scientific Conference CONFSEC ISSN print 2603-2945, ISSN online 2603-2953, year 1, ISSUE 2(2), 2017, Avaible from http://confsec.eu/sbornik/1-2017.pdf