УДК 004.056

И.В. Лысенко, Ю.В. Трегуб

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ВОЗМОЖНОСТЕЙ ПРОГРАММНЫХ ПЛАТФОРМ И ЯЗЫКОВ ПРОГРАММИРОВАНИЯ С ТОЧКИ ЗРЕНИЯ РЕАЛИЗАЦИИ КРИПТОАЛГОРИТМОВ

Проанализированы одни из наиболее популярных программных платформ и языков программирования в отношении возможностей реализации криптографических алгоритмов обеспечения конфиденциальности (симметричные и несимметричные алгоритмы шифрования), целостности и аутентичности данных (ключевые и бесключевые хеш-функции и алгоритмы цифровой подписи), а также протоколов формирования сеансовых ключей пользователей. Результаты сравнительного анализа могут служить основой для принятия решения пользователю в отношении создания собственной подсистемы криптозащиты данных.

Ключевые слова: *криптоалгоритмы, программные платформы, языки программирования.*

Введение

Постановка задачи. С увеличением объёма циркулирующей в открытых сетях информации, а также информации, хранящейся на жёстком диске пользователя, возрастает актуальность задачи её защиты.

Часто данная задача решается преимущественно за счёт применения программно-реализованных криптографических алгоритмов, позволяющих обеспечить такие свойства защищаемых данных, как конфиденциальность, целостность и аутентичность. К числу других важных задач, решаемых криптографическими алгоритмами, относится задача формирования сеансовых ключей удалённых пользователей.

Существующие программные платформы и языки программирования позволяют пользователю реализовать подсистему криптозащиты данных на основе встроенных библиотек криптоалгоритмов (криптопримитивов). Так, в [1, 2] приводятся данные об используемых в одних из наиболее популярных платформ (MS .Net Framework и Java) алгоритмов шифрования.

Что же касается языков программирования, то в данной работе рассматриваются, PHP, Python, C++, Delphi. При этом, хотя Delphi никак нельзя относить к числу наиболее популярных языков, он выбран для сравнительного анализа с точки зрения широты рассмотрения вопроса.

В [7, 8] содержится перечень криптоалгоритмов, используемых в некоторых из вышеперечисленных языков программирования.

Целью работы является анализ упомянутых программных платформ и языков программирования с точки зрения возможности реализации криптопримитивов.

1. Возможности программных платформ

Возможности программных платформ по реализации криптопримитивов представлены в табл. 1 [3, 4].

Таблица 1

Возможности платформ .Net Framework и Java

Криптопримитивы	Программная платформа	
	.Net Framework	Java
Симметричное шифрование	AES, DES, 3DES, RC2, RC4	AES, DES, DESede, RC2, RC5, RC4, IDEA, Blowfish
Несимметричное шифрование	RSA	RSA, El-Gamal
Цифровая подпись	RSA, DSA, ECDSA	RSA, DSA, ECDSA
Бесключевые хеш-функции	MD5, SHA-1, SHA256, SHA384, SHA512	MD2, MD5, SHA-1, SHA-256 SHA-384 SHA-512
Ключевые хеш-функции	MACTrileDES, HMAC	HMAC-SHA1

Как видно из табл. 1, наибольшим набором криптопримитивов среди программных платформ обладает Java. В частности, что касается симметричных алгоритмов шифрования, в Java, помимо алгоритмов, реализованных в .Net Framework, присутствуют блочные криптоалгоритмы RC5 и Blowfish, а также потоковые алгоритмы RC4 и Arcfour (в .Net Framework потоковые алгоритмы отсутствуют). Кроме того, в Java имеется возможность реализации несимметричного алгоритма шифрования Эль-Гамаля (кроме RSA), в то время как в .Net Frame-

work несимметричное шифрование представлено только алгоритмом RSA. Помимо этого Java позволяет реализовать гибридную схему шифрования на основе эллиптических кривых ECIES. Криптопримитивы цифровой подписи в платформах .Net Framework и Java представлены одним и тем же набором алгоритмов.

Что касается бесключевых хеш-функций, то их набор в программной платформе Java является практически идентичным набору в .Net Framework, за исключением того, что в Java реализована хеш-функция MD2 (не используется, как криптопримитив). В отношении ключевых хеш-функций платформа .Net Framework обладает такими алгоритмами хеширования, как MACTripleDES и HMAC, в то время как в Java используется лишь криптопримитив HMAC-SHA1.

Также следует отметить, что рассматриваемые платформы позволяют реализовать протокол Диффи-Хеллмана формирования общего секретного ключа пользователей на основе эллиптических кривых (ECDiffieHellman).

2. Возможности языков программирования

Возможности языков программирования по реализации криптопримитивов представлены в табл. 2.

Как видно из табл. 2, наибольшим набором криптопримитивов среди рассмотренных языков программирования обладает язык C++.

В отличие от других языков программирования, несимметричное шифрование в нём представлено не только алгоритмом RSA, но и алгоритмом шифрования Эль-Гамаля. Возможность реализации данного алгоритма присутствует и в платформе Java. Особенностью языка C++ с точки зрения симметричного блочного шифрования является то, что в нём, помимо множества алгоритмов семейства RC (автор – всемирно известный криптолог Рональд Райвест), представлены оба алгоритма ещё одного всемирно известного криптолога Брюса Шнайера Blowfish и Twofish. В то же время, в C++ отсутствует реализация симметричного поточного шифрования, представленного в языках Delphi и PHP алгоритмом RC4.

Также в языках C++ и Python, в отличие от других языков, имеется реализация гибридной схемы шифрования ECIES, использующей математический аппарат эллиптических кривых.

Если говорить о цифровой подписи, то набор криптопримитивов в языке программирования C++ идентичен языку Delphi, и содержит, помимо реализованных в других языках (за исключением PHP) алгоритмов RSA и DSA, алгоритм на эллиптических кривых ECDSA.

Таблица 2

Возможности языков программирования

Криптопримитивы	Языки программирования			
	Delphi	PHP	C++	Python
Симметричное шифрование	AES, DES, 3DES, IDEA, RC2, RC4, RC5, RC6, XOR	AES, DES, Blow-fish, RC4	AES DES, 3DES, IDEA, RC2, RC5, RC6, Blowfish, Twofish	AES, DES, 3DES, XOR
Несимметричное шифрование	RSA	RSA	RSA, ElGamal, ECIES	RSA ECIES
Цифровая подпись	RSA, DSA, ECDSA	RSA	RSA, DSA, ECDSA	RSA, DSA
Бесключевые хеш-функции	MD4, MD5, SHA-1, SHA256 SHA384 SHA512	MD5 SHA-1 SHA-256	MD2, MD4, MD5, SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 SHA-3	MD2, MD4, MD5, SHA-1, SHA-256, SHA-384, SHA-512
Ключевые хеш-функции	HMAC-SHA-1, HMAC-SHA256	HMAC-MD5	HMAC	HMAC

Что касается бесключевых хеш-функций, то во всех рассмотренных языках, помимо практически вышедших из употребления алгоритмов семейства MD и SHA-1, реализовано семейство хеш-функций SHA-2 с длиной дайджеста 224, 256, 384 и 512 битов. Однако в языке программирования C++ также поддерживается и бесключевая хеш-функция SHA-3. Ключевые хеш-функции во всех рассматриваемых языках представлены схемой HMAC на основе разных бесключевых хеш-функций.

В целом же, что касается языков программирования, важно заметить тот факт, что реализация протокола Диффи-Хеллмана формирования общего секретного ключа пользователей на основе эллиптических кривых (ECDiffieHellman), присутствует не только в языке программирования C++, но и в практически вышедшем из употребления языке Delphi, который, как можно видеть, почти не уступает C++

с точки зрения разнообразия реализованных криптопримитивов.

Следует отметить, что возможность реализации протокола Диффи-Хеллмана присутствует и в платформах .Net Framework и Java.

Заключение

Результаты проведенного анализа позволяют пользователю, желающему реализовать собственную подсистему криптозащиты данных, иметь представление о возможностях программных платформ и языков программирования с точки зрения реализации базовых криптопримитивов и осуществлять выбор программной системы на основе собственных предпочтений и навыков программирования. В частности, что касается производительности криптоалгоритмов реализованных в .Net Framework, результаты соответствующих исследований, опубликованы в [7, 8].

Список литературы

1. Java Cryptography Architectur Standard Algorithm Name Documentation for JDK 8 [Электронный ресурс] / Oracle.com – Режим доступа: https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html .

2. Msdn.microsoft.com, .NET Framework Cryptography Model [Электронный ресурс] / Msdn.microsoft.com – Режим доступа : https://msdn.microsoft.com/enus/library/0ss79b2x(v=vs.110).aspx.

3. Wikipedia.org . Crypto++ [Электронный ресурс] / Wikipedia.org – Режим доступа: https://en.wikipedia.org/wiki/Crypto%2B%2B .

4. Efg2.com, Cryptography and Multiple-Precision Arithmetic [Электронный ресурс] / Efg2.com – Режим доступа: http://www.efg2.com/Lab/Library/Delphi / MathFunctions/Cryptography.htm.

5. Авдошин, С.М. Криптотехнологии Microsoft / С.М. Авдошин, А.А. Савельева // Приложение к журналу «Информационные технологии» – 2008. – №9. – С. 23–30.

6. Смарт, Н. Криптография: пер. с англ. / Н. Смарт – М.: Техносфера, 2005. – 528 с.

7. Лысенко, И.В. Исследование быстродействия алгоритмов шифрования на базе технологии .Net Framework / И.В Лысенко, А.Г.Проценко, // Системи обробки інформації / ХУПС. – Х., 2011. – Вип. 4(94). – С. 176-181.

8. Проценко, А.Г. Исследование быстродействия алгоритмов обеспечения целостности на базе технологии .Net Framework / А.Г.Проценко // Системи обробки інформації: ХУПС. – Х.в, 2011. – Вип. 8(52). – С. 228-232.

References

1. "Java Cryptography Architecture Standard Algorithm Name Documentation for JDK 8", available at: https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html .

2. ".NET Framework Cryptography Model, available at: https://msdn.microsoft.com/enus/library/0ss79b2x (v=vs.110).aspx .

3. "Crypto++", available at: https://en.wikipedia.org/wiki/Crypto%2B%2B .

4. "Cryptography and Multiple-Precision Arithmetic", available at: http://www.efg2.com/Lab/Library/ Delphi/MathFunctions/Cryptography.htm.

5. Avdoshin, S.M., Savel'eva, A.A. (2008), "Microsoft Cryptotechnologies" [Kriptotehnologii Microsoft], Prilozhenie k zhurnalu «Informacionnye tehnologii», no.9, pp. 23–30.

6. Smart, N. (2005), Cryptography, Trans. from Russ. ed.: [Kriptografija, Per. s Russ. ed], Tehnosfera Publ. 528 p.

7. Lysenko, I.V., Procenko, A.G.(2011), "Speed encryption algorithm study based on .Net Framework technology", Information processing systems ["Issledovanie bystrodejstvija algoritmov shifrovanija na baze tehnologii .Net Framework", Sistemi obrobki informacii], HUPS, Kharkiv, Vol. 4(94). pp. 176-181.

8. Procenko, A.G., (2011), "Research performance integrity algorithms based on the .Net Framework technology", Information processing systems ["Issledovanie bystrodejstvija algoritmov obespechenija celostnosti na baze tehno-logii .Net Framework", Sistemi obrobki informacii], HUPS, Kharkiv, Vol. 8(52). pp. 228-232.

Надійшла до редколегії 3.02.2017

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА МОЖЛИВОСТЕЙ ПРОГРАМНИХ ПЛАТФОРМ І МОВ ПРОГРАМУВАННЯ З ТОЧКИ ЗОРУ РЕАЛІЗАЦІЇ КРИПТОАЛГОРИТМІВ

І.В. Лисенко, Ю.В. Трегуб

Проаналізовано деякі найбільш популярні програмні платформи і мови програмування щодо можливостей реалізації криптографічних алгоритмів забезпечення конфіденційності (симетричні і несиметричні алгоритми шифрування), цілісності й автентичності даних (ключові і бесключові хеш-функції та алгоритми цифрового підпису), а також протоколів формування сеансових ключів користувачів. Результати порівняльного аналізу можуть бути основою для прийняття рішення користувачеві з питання створення власної підсистеми криптографічного захисту даних.

Ключові слова: *криптоалгоритми, програмні платформи, мови програмування.*

COMPARATIVE CHARACTERISTICS OF OPPORTUNITIES SOFTWARE PLATFORMS AND PROGRAMMING LANGUAGES IN TERM OF IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS

I.V. Lysenko, J.V. Tregub

Some of the most popular software platform and programming language were analyzed regarding the feasibility of cryptographic algorithms ensure confidentiality (symmetric encryption and asymmetric encryption algorithms), the integrity and authenticity of data (key hash, keyless hash function, and digital signature algorithms), and protocols form of session keys of users. Results of comparative analysis can serve as the basis for a user who makes a decision regarding the establishment of its own data encryption subsystem.

Keywords: *cryptographic algorithms, software platforms, programming languages .*