УДК 004.056:004.6

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ШИФРОВАНИЯ БОЛЬШИХ ДАННЫХ В СИСТЕМАХ ВИДЕО И АУДИО СВЯЗИ

Шибко И.А.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Телеш И.А. – канд. геогр. наук, доцент, доцент кафедры ИПиЭ

Аннотация. Рассмотрены различные методы шифрования: симметричное, гомоморфное, потоковое, используемые в системах видео и аудио связи. Приводятся примеры реализации этих методов: AES, DES, RSA и RTMP.

Ключевые слова: AES, DES, RSA, RTMP, реализации шифрования, безопасность данных, симметричное шифрование, гомоморфное шифрование, потоковое шифрование.

Введение. Системы видео и аудио связи сегодня играют ключевую роль в медиа-, телекоммуникациях и видеоконференциях. В медиакоммуникациях они обеспечивают высококачественное вещание и стриминг контента. В телекоммуникациях они поддерживают надежную связь на любом расстоянии. В видеоконференциях они позволяют проводить встречи в режиме реального времени. Подобные системы продолжают совершенствоваться в области коммуникаций и медиа [1]. При этом важным аспектом является обеспечение безопасности и конфиденциальности в ходе проведения видео- и аудио- конференций. Одной из основных проблем является риск утечки конфиденциальной информации. А также существует проблема несанкционированного доступа к видео- и аудиоданным [2, 3]. Для решения этих проблем требуется повышение мер безопасности с использованием надежных методов шифрования.

Основная часть. Стриминг – это технология передачи данных в реальном времени по сети интернет, позволяющая пользователям просматривать или слушать контент без необходимости его полной загрузки на устройство. Видео- и аудио-конференции - специализированные виды стриминга, где участники могут общаться в реальном времени через видео и звуковые потоки. Существуют различные методы шифрования, которые применяются в данных системах.

Симметричное шифрование использует один и тот же ключ для шифрования и дешифрования данных. Это эффективный метод для обработки больших объемов данных, но при этом требует безопасного способа передачи ключа [4]. Визуальное представление симметричного шифрования показано на рисунке 1.

Потоковое шифрование – это метод шифрования, который преобразует исходный текст в код. Потоковые шифры линейны, поэтому один и тот же ключ шифрует и дешифрирует сообщения [5]. Визуальное представление потокового шифрования показано на рисунке 2.

Рисунок 1 – Схема работы симметричного шифрования

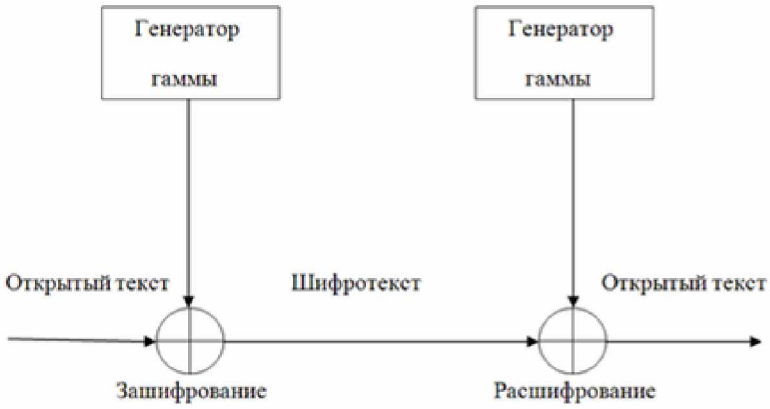

Рисунок 2 – Схема работы потокового шифрования

Гомоморфное шифрование – инновационная технология, которая позволяет выполнять вычисления над зашифрованными данными без их предварительного дешифрования, но из-за большого размера зашифрованных пакетов данных и необходимости их дальнейшей расшифровки данный метод требователен к вычислительным ресурсам [6].

Примерами реализации этих видов шифрования являются: AES (Advanced Encryption Standard) и DES (Data Encryption Standard) для симметричного шифрования, RSA (Rivest–Shamir–Adleman) для гомоморфного шифрования, AES 128 и RTMP (Real Time Messaging Protocol Streaming) для потокового шифрования.

AES (Advanced Encryption Standard): симметричный блочный шифр, используемый для шифрования и дешифрования информации. AES использует ключи разной длины (128, 192, 256 бит) для шифрования и дешифрования данных блоками по 128 бит [7]. Схема работы AES предоставлена на рисунке 3.

DES (Data Encryption Standard) – симметричный блочный шифр, я является одним из первых стандартов шифрования, принятых в качестве официального стандарта шифрования в [8]. Схема работы DES предоставлена на рисунке 4.

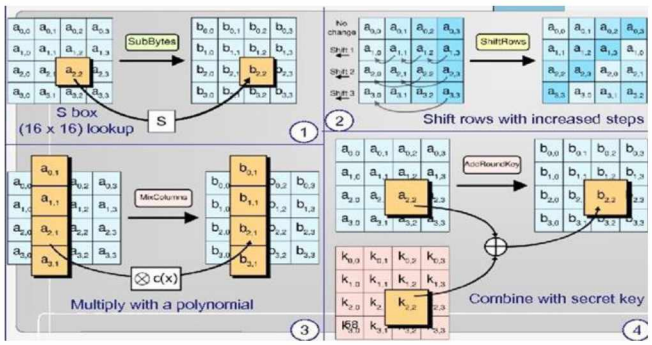

Рисунок 3 – Схема работы AES

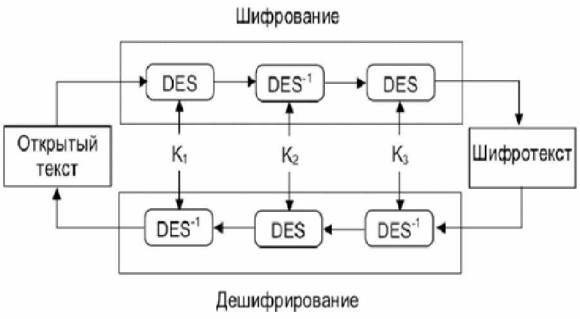

Рисунок 4 – Схема работы DES

RSA (Rivest–Shamir–Adleman) – асимметричная криптосистема, которая поддерживает гомоморфное шифрование. Она позволяет выполнять операции умножения на зашифрованных данных [9]. Схема работы RSA предоставлена на рисунке 5.

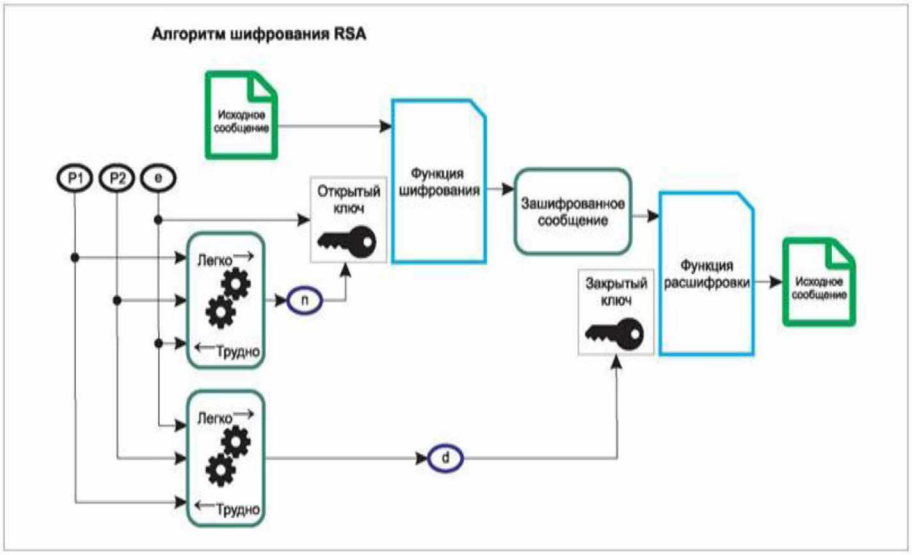

Рисунок 5 – Схема работы RSA

AES-128 (Advanced Encryption Standard 128) – симметричный блочный шифр, который широко используется для потокового шифрования [10]. Схема работы AES-128 показана рисунке 6.

RTMP (Real Time Messaging Protocol Streaming) – метод шифрования, используемый для защиты потокового контента [10]. Схема работы RTMP показана на рисунке 7.

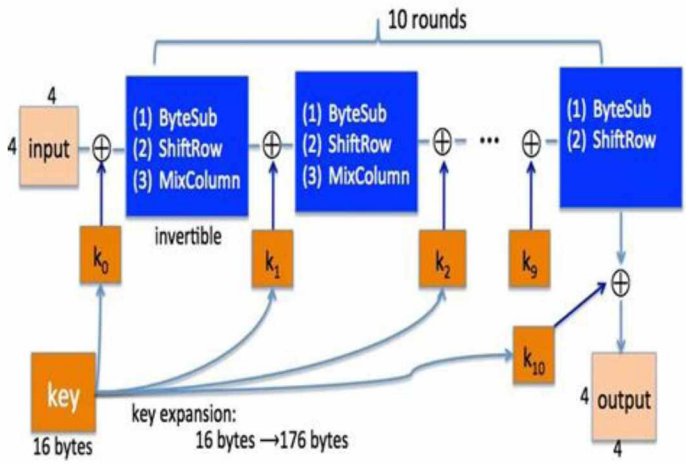

Рисунок 6 – Схема работы AES-128

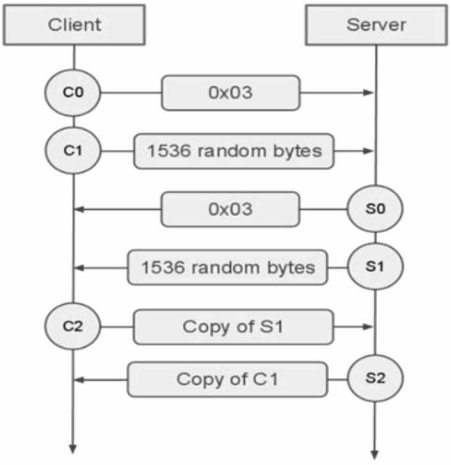

Рисунок 7 – Схема работы RTMP

Заключение. Применение технологий шифрования в системах видео и аудио связи является важным и необходимым шагом в обеспечении безопасности и конфиденциальности данных в цифровом пространстве. Новые методы шифрования позволяют минимизировать угрозу при передаче данных, противостоять развитию киберпреступности, а постоянное развитие технологий позволяет использовать более совершенные методы шифрования.

Список литературы

1. Professional Audio Visual Systems Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029) [Электронный ресурс] – Режим доступа: https://www.mordorintelligence.com/industry-reports/professional-audio-visual-systems-market. – Дата доступа 09.02.2024

2. Security Concerns and Citizens' Privacy Implications in Smart Multimedia Applications [Электронный ресурс] – Режим доступа: https://www.springerlink.com/content/123456789/. – Дата доступа 10.02.2024.

3. Security and Privacy in Video Surveillance: Requirements and Challenges [Электронный ресурс] – Режим доступа: https://www.springerlink.com/content/987654321/. – Дата доступа 10.02.2024.

4. Difference between Symmetric and Asymmetric Key Encryption [Электронный ресурс] – Режим доступа: https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/. – Дата доступа 10.02.2024.

5. Homomorphic Encryption [Электронный ресурс] – Режим доступа: https://en.wikipedia.org/wiki/Homomorphic_encryption. – Дата доступа 10.02.2024.

6. Stream Cipher [Электронный ресурс] – Режим доступа: https://www.okta.com/identity-101/stream-cipher/. – Дата доступа 10.02.2024.

7. Symmetric Encryption Techniques [Электронный ресурс] – Режим доступа: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:data-encryption-techniques/a/symmetric-encryption-techniques. – Дата доступа 10.02.2024.

8. Symmetric Key Encryption: Why, Where and How It's Used in Banking [Электронный ресурс] – Режим доступа: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking. – Дата доступа 10.02.2024.

9. Homomorphic Encryption [Электронный ресурс] – Режим доступа: https://en.wikipedia.org/wiki/Homomorphic_encryption. – Дата доступа 10.02.2024.

10. Video Encryption Protection [Электронный ресурс] – Режим доступа: https://www.vdocipher.com/blog/2020/08/video-encryption-protection/. – Дата доступа 10.02.2024.

UDC 004.056:004.6

APPLICATION OF ENCRYPTION TECHNOLOGIES IN VIDEO AND AUDIO COMMUNICATION SYSTEMS

Shybko I.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Telesh I.A. – Cand. of Sci., Associate Professor of the Department

Annotation: Various encryption methods are considered: symmetric, homomorphic, streaming, used in video and audio communication systems. Examples of implementation of these methods are given: AES, DES, RSA and RTMP.

Keywords: AES, DES, RSA and RTMP – methods for implementing encryption of video and audio communications, data security, symmetric encryption, homomorphic encryption, stream encryption.