УДК 004.056.55

А. В. Приймак

ПІДВИЩЕННЯ ЗАХИСТУ ОБМІНУ ДАНИМИ В ЛОКАЛЬНІЙ МЕРЕЖІ

Вінницький національний технічний університет

Анотація

В роботі розглянуто проблему захищеної передачі даних в локальній мережі, а також підвищено якість захисту за допомогою криптографічного алгоритму Cramer-Shoup. Згідно даного шифру розроблено програму — текстовий чат, що забезпечує надійний захист при обміні інформацією між користувачами в локальній мережі.

Ключові слова: локальна мережа, криптографія, Cramer-Shoup, крипточат.

Abstract

In the paper the problem of secure data transmission in the local network is considered, as well as the quality of protection with the help of cryptographic algorithm Cramer-Shoup. According to this cipher, a program has been developed - a text chat that provides reliable protection in the exchange of information between users on the local network.

Keywords: local area network, cryptography, Cramer-Shoup, cryptochat.

Вступ

В наш час питання захисту інформації стало невід'ємною частиною любої системи яка працює з комерційно значущою інформацією. При вільному обміні інформацією в локальних мережах виникають проблеми її захищеності, а також обмеження доступу зовнішніх користувачів до цих мереж. Захист інформації стоїть на першому місці по актуальності і постановці задач. На сьогоднішній день, в більшості локальних мережах, обмін інформацією відбувається за рахунок спілкування в різноманітних месенджерах та чатах, тому підвищення захисту обміну даними в локальній мережі є дійсно актуальним. Провівши аналіз існуючих крипточатів, було зроблено висновок, що вони далекі від ідеалів захищеної передачі даних та зручності у використанні звичайними користувачами. Більшість з них є фінансово неефективними, обмін інформацією є не зручним для звичайних користувачів локальної мережі, а деякі з використаних технологій є застарілими на даний момент, оскільки більшість з вище наведених месенджерів використовують криптографічний алгоритм RSA для захищеної передачі даних, але на даний момент він є застарілим з безліччю відомих на нього атак та недоліків.

Результати дослідження

Запропонований крипточат використовує криптосистему з публічним ключем Cramer-Shoup для надійного обміну повідомленнями між користувачами. Загальна схема процесу шифрування та дешифрування зображена на рисунку 1.

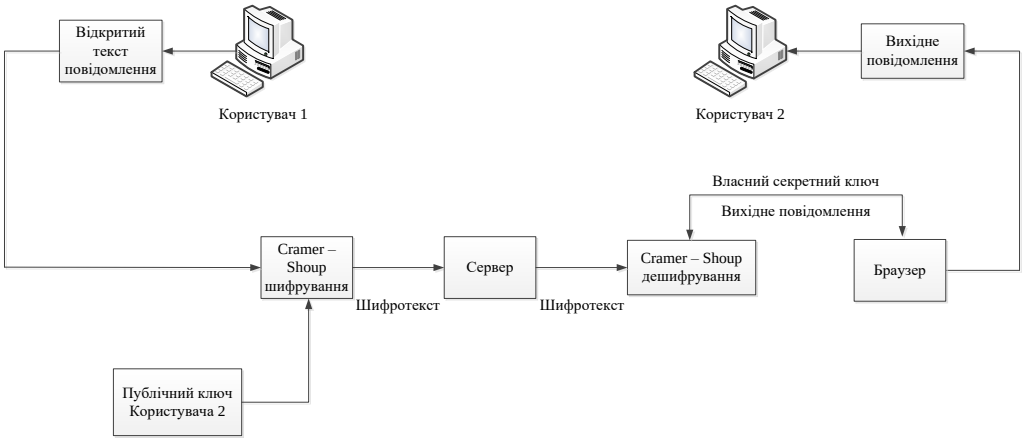

Рисунок 1 – Процес шифрування та дешифрування повідомлення

Процес шифрування та дешифрування повідомлення має такий вигляд:

1. Два клієнта підключаються до сервера.

2. Після підключення, кожному клієнту автоматично генеруються свої публічні та приватні ключі локально.

3. При передачі повідомлення воно попередньо шифрується за допомогою публічного ключа.

4. На стороні іншого користувача відбувається зворотна операція. За допомогою відомого публічного ключа та персонального секретного ключа, сервер дешифрує надіслане повідомлення.

Після підключення користувача до чату йому генеруються публічний та секретний ключ.

Публічний ключ зберігається на сервері та є видимим для 2 користувачів. Також варто зазначити, що публічні ключі не зберігаються в базі даних, а зберігаються у виконуваному файлі і діють лише під час сесії чату користувачів, для яких вони і були згенеровані.

В свою чергу, секретні ключі зберігаються в куках браузера. Оскільки це веб-браузерний крипто чат, то для забезпечення захищеного зберігання та використання секретних ключів, вони зберігаються у тимчасовому хранилищі даних веб-браузера для певної сторінки, в даному випадку чату. У цьому разі, можлива втрата секретного ключа або його перехоплення зловмисником відсутня при використанні HTTPs протоколу для обміну запитами та інформацією між браузером та сервером. Час дії збереженого секретного ключа в браузері становить 1 день, після чого з'єднання автоматично розірветься і вся переписка знищиться.

Висновки

Отже запропонована схема ефективно реалізує захищений обмін інформацією між користувачами в локальній мережі, а криптографічний алгоритм Cramer-Shoup являється кращою заміною сучасних використовуваних алгоритмів, оскільки він є захищеним від адаптивної вибраної атаки шифру тексту за допомогою стандартних криптографічних припущень, а його криптостійкість і швидкість роботи вище ніж у RSA та ElGamal.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Local area network [Electronic Resource]. – Mode of access : URL : https://en.wikipedia.org/wiki/Local_area_network. - Назва з екрану.
2. Яремчук Ю. Є. Алгебраїчні моделі асиметричних криптографічних систем / Юрій Євгенович Яремчук. // Захист інформації. – 2014. – №16. – С. 68–80.
3. Public-key cryptography [Electronic Resource]. – Mode of access : URL : https://en.wikipedia.org/wiki/Public-key_cryptography. - Назва з екрану.
4. Cryptochat [Electronic Resource]. – Mode of access : URL : https://uk.wikipedia.org/wiki/Cryptocat. - Назва з екрану.
5. Cramer-Shoup cryptosystem [Electronic Resource]. – Mode of access : URL : https://en.wikipedia.org/wiki/Cramer%E2%80%93Shoup_cryptosystem. - Назва з екрану.

Приймак Андрій Васильович — аспірант, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: andrii.pryimak@live.com.

Науковий керівник: ***Яремчук Юрій Євгенович*** — доктор технічних наук, професор, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.

Pryimak Andrii Vasyliovych — postgraduate, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, e-mail: andrii.pryimak@live.com.

Supervisor: ***Yaremchuk Yuriy E***. — D. Sc., professor, management and security of information Systems department; Vinnitsa.