DOI: https://doi.org/10.32836/2521-6643-2019-1-57-7
УДК 004.056.55

Л. В. Кабак, кандидат технічних наук, доцент кафедри програмного забезпечення комп'ютерних систем Національного технічного університету "Дніпровська політехніка"
О. Н. Молотков, кандидат технічних наук, доцент кафедри інформаційних систем та технологій Університету митної справи та фінансів
О. П. Буланий, кандидат фізико-математичних наук, доцент кафедри інформаційних систем та технологій Університету митної справи та фінансів
В. В. Куц, студент Університету митної справи та фінансів

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ВБУДОВАНИХ ПАКЕТІВ КРИПТОЗАХИСТУ ДАНИХ СЕРВЕРІВ MS SQL SERVER ТА ORACLE

Проведено дослідження, розглянуто можливості впровадження вбудованих у сервер Oracle та MS SQL Server алгоритмів криптозахисту даних у спеціалізовані інформаційні системи на прикладі інформаційної системи Державної фіскальної служби України. Досліджено швидкодію роботи алгоритмів, оцінено зростання завантаження серверів і навантаження на комп'ютерну мережу через збільшення обсягу даних, що передаються. Набув подальшого розвитку метод оцінювання роботи вбудованих симетричних алгоритмів шифрування даних. Запропоновано алгоритм універсальної функції, яка дає можливість шифрувати дані завдяки введеному ключеві та обраному алгоритму.

Ключові слова: *криптоалгоритми; захист даних; шифрування даних; бази даних; спеціалізовані інформаційні системи.*

Проведено исследование и рассмотрены возможности внедрения встроенных в сервер Oracle и MS SQL Server алгоритмов криптозащиты данных в специализированные информационные системы на примере информационной

системы Государственной фискальной службы Украины. Также исследовано быстродействие работы алгоритмов и проведена оценка роста загрузки серверов и нагрузка на компьютерную сеть за счет увеличения объемов передаваемых данных. Получил дальнейшее развитие метод оценки работы встроенных симметричных алгоритмов шифрования данных. Предложен алгоритм универсальной функции, которая позволяет проводить шифрование данных благодаря введенному ключу и выбранному алгоритму.

Ключевые слова: *криптоалгоритмы; защита данных; шифрование данных; базы данных; специализированные информационные системы.*

At the present time Oracle and MS SQL Servers are used for datastorage in the information system of department of customs control organization and for processing of State Fiscal Service of Ukraine. Data cumulated during customs clearance which requires access from all users are spread among many databases located between various physical storages. Data is passed between servers using different types of computer networks. With development of ramified informational systems and networks become a topical issue of ensuring sustainability, confidentiality and authenticity of data in customs departments of fiscal service of Ukraine, which are transmitted through open data line, through usage of modern cryptography methods. It's important to know that there are different methods that help to choose such set of security tools that will provide maximum data security. To protect data from unauthorized access are used modern data encryption algorithms. At the present time data is transmitted over the computer network without usage of any crypt protection system which may give attacker opportunity to capture data. DBMS Oracle and MS SQL Server have standard built-in crypto data protection packets. The purpose of this article is to consider merits and demerits of using these packages and analyze possibility of their using in customs departments of fiscal service of Ukraine. According to research technique in this article following tasks were solved: analyzing of built-in crypto data protection packets, as in their cryptostability, speed and volume increase of transmitted data, developing of plug-in for speed test of existing methods for crypt protection, considering possibility of implementation built-in packets into informational system of fiscal service of Ukraine. In this article, the speed of algorithms work was investigated and an estimation of the growth of server loading and loading on the computer network was made due to the increase of data vo-lumes being transmitted. In the article, the method for evaluating the work of embedded symmetric data encryption algorithms has been further developed.

Key words: *grid system; partitioning; data consolidation; data bases; specialized information systems.*

Постановка проблеми. Нині в інформаційній системі департаменту організації митного контролю та оформлення Державної фіскальної служби України для збереження даних використовують сервери Oracle та MS SQL Server. Дані, що накопичуються під час митного оформлення, до яких необхідний доступ усім користувачам, розкидані серед безлічі баз даних, розташованих у різних фізичних місцях зберігання. Дані передаються між серверами через різні типи комп'ютерних мереж. Із розвитком розгалужених інформаційних систем і мереж стало актуальним питання забезпечення цілісності, конфіденційності та достовірності даних в митних підрозділах Державної фіскальної служби України, які передаються через відкриті канали зв'язку, шляхом використання сучасних методів криптографії. Важливо знати, що існують різні методи, котрі допомагають обрати таку сукупність засобів захисту, яка забезпечить максимальну безпеку даних. Для захисту даних від несанкціонованого доступу використовують сучасні алгоритми шифрування даних. Деякі стандартні алгоритми у вигляді пакетів постачаються разом із СКБД Oracle та MS SQL Server. Для організації роботи сучасної Єдиної інформаційної системи фіскальної служби використовуються засоби Oracle, які називаються розподіленою базою даних і тиражуванням даних. Кожна база даних керується власною локальною системою керування базою даних (далі – СКБД). Усі сервери баз даних у розподіленій базі даних співпрацюють, щоб підтримувати погодженість глобальної бази даних. Однак нині дані передаються через комп'ютерну мережу без використання будь-яких систем криптозахисту, це уможливлює перехоплення даних зловмисниками. СКБД Oracle має утиліту Oracle Advanced Security, яку потрібно купувати за окремі кошти, але вона не придатна для роботи гетерогенних розподілених баз даних. СКБД Oracle та MS SQL Server мають стандартні вбудовані пакети криптозахисту даних. Мета дослідження – розглянути переваги та недоліки використання цих пакетів, а також можливість їх використання в митних підрозділах фіскальної служби України.

Відповідно до мети наукового дослідження слід виконати такі завдання:

– вивчити вбудовані пакети криптозахисту даних, а саме: їхню криптостійкість, швидкодію та збільшення обсягу даних, що передаються;

– розробити алгоритм тестування швидкодії наявних методів криптозахисту;

– розглянути можливість втілення убудованих пакетів в інформаційну систему Державної фіскальної служби України.

Аналіз останніх досліджень і публікацій. У СКБД Oracle та MS SQL Server наявні такі алгоритми шифрування даних: DES, DES3, AES.

DES (англ. Data Encryption Standard) – це симетричний алгоритм шифрування певних даних, стандарт шифрування прийнятий урядом США з 1976 р. до кінця 1990-х рр., із часом набув міжнародного застосування. Ще

після розроблення алгоритм викликав неоднозначні відгуки. Оскільки DES містив засекречені елементи своєї структури, то виникали побоювання щодо можливості контролю з боку Національного Агентства Безпеки США (англ. National Security Agency). Алгоритм піддавався критиці через малу довжину ключа, що, зрештою, після бурхливих обговорень і контролю академічної громадськості не завадило йому стати загальноприйнятим стандартом. DES дав поштовх сучасним уявленням про блокові алгоритми шифрування та криптоаналіз [1–3].

Нині DES вважається ненадійним, адже він має малу довжину ключа (56 біт) і розмір блоку (64 біти). У праці M. Mitsuru [4] подано методику криптоаналізу, завдяки якій у 1999 р. ключ DES було публічно дешифровано. Процес дешифрування тривав 22 год 15 хв. Нині цей алгоритм використовується в модифікації 3-DES, вважається, що в цій модифікації алгоритм досить надійний для застосування. DES поступово витісняється алгоритмом AES, що з 2002 р. є стандартом США [2; 4].

Робота над розробкою алгоритму шифрування AES почалась 1997 р. у NIST (National Institute of Standards and Technology). Співробітники цього інституту співпрацювали з промисловцями та вченою спільнотою, котра займалась криптозахистом інформації, й досліджували новітні методи для розробки сучасного більш надійного, вдосконаленого стандартного стандарту шифрування. Мета полягала в тому, щоб розробити алгоритм шифрування, який можна використовувати як стандартний алгоритм шифрування. І цей алгоритм було зараховано до Федерального стандарту обробки інформації (далі – FIPS). Вважається, що він має достатню криптостійкість і зможе добре захистити інформацію уряду та інших організацій упродовж досить тривалого проміжку часу. Нині цей алгоритм використовує уряд США та на добровільних засадах будь-які підприємства. Крім того, цей алгоритм реалізовує симетричну криптографію ключів як блоковий шифр, він підтримує розміри блоків 128 біт і розмір ключів 128, 192, 256 біт [5–8].

Мета статті – дослідження можливості використання вбудованих у СКБД Oracle та MS SQL Server криптографічних алгоримів захисту інформації на швидкодію, розмір даних, які отримуються після шифрування даних, і криптостійкість. Для тестування вбудованих алгоритмів розроблено спеціальний програмний додаток, за допомогою якого проводились експерименти.

Виклад основного матеріалу. В сучасній Єдиній автоматизованій інформаційній системі митних підрозділів Державної фіскальної служби України використовуються СКБД ORACLE та MS SQL Server.

У СКБД Oracle та MS SQL Server наявні такі алгоритми шифрування даних: DES, DES3, AES. Для реалізації цих алгоритмів використовується

пакет DBMS_CRYPTO. Опис функцій, що зараховуються до пакета, подано в табл. 1. Пакет DBMS_CRYPTO надає тільки одну функцію для шифрування даних, саме тому тип шифрування зазначається в параметрі. Алгоритми шифрування, що підтримуються, та відповідні їм функції подано в табл. 1. Необхідна константа задається у форматі *ім'я_пакета.ім'я_функції*. Наприклад, щоб обрати алгоритм Triple DES, слід використовувати функцію DBMS_CRYPTO.ENCRYPT_3DES.

Таблиця 1

Алгоритми шифрування пакета DBMS_CRYPTO

Ім'я_функції	Опис	Довжина ключа, Bit
ENCRYPT_DES	Data Encryption Standard (DES)	56
ENCRYPT_3DES_2KEY	Modified Triple Data Encryption Standard обробляє кожен блок тричі, використовуючи 2 ключі	112
ENCRYPT_3DES	Triple Data Encryption Standard (3DES); обробляє кожен блок тричі	156
ENCRYPT_AES128	Advanced Encryption Standard	128
NCRYPT_AES192	Advanced Encryption Standard	192
ENCRYPT_AES256	Advanced Encryption Standard	256
ENCRYPT_RC4	Потокове шифрування	

Під час застосування пакета слід обрати алгоритм шифрування, задавши відповідне значення параметра *typ*. Під час шифрування даних кожен блок, який зашифровується, може бути зашифрований незалежно від інших або зчеплений з іншими для створення більш надійної (з погляду криптографії) системи. В останньому випадку зашифроване значення краще захищено. Щоб обрати метод зчеплення, слід зазначити відповідну константу з табл. 2 у значенні параметра *typ*, наприклад DBMS_CRYPTO.CHAIN_OFB.

Під час використання алгоритмів шифрування слід явно доповнити дані так, щоб їхня довжина була кратна розміру блоку. Однак цей підхід не є криптографічно надійним. DBMS_CRYPTO дає змогу вказати необхідний тип доповнення. Більшість компаній використовує метод PKCS # 5 [9].

Щоб обрати метод доповнень, слід зазначити відповідну константу з табл. 3 у значенні параметра *typ,* DBMS_CRYP TO.PAD_PKCS5.

Таблиця 2

Типи зчеплень DBMS_CRYPTO

Константа	Опис
CHAIN_CBC	Зчеплення блоків шифротексту – Cipher Block Chaining
CHAIN_ECB	Електронна книга кодів – Electronic Code Book
CHAIN_CFB	Шифрування зі зворотним зв'язком від шифротексту – Cipher Feedback
CHAIN_OFB	Шифрування зі зворотним зв'язком за виходом – Output Feedback

Таблиця 3

Типи доповнення DBMS_CRYPTO

Константа	Опис
PAD_PKCS5	Доповнення засобами криптографічної системи із загальним ключем (Public Key Cryptography System # 5)
PAD_ZERO	Доповнення нулями
PAD_NONE	Відсутність доповнення. Використовується в разі впевненості в тому, що довжина даних уже кратна розміру блоку, що зашифровується (кратно 8)

Нині на митних постах для митного оформлення використовується ПІК "Інспектор 2006", тому дані зберігаються у СКБД MS SQL Server. У СКБД MS SQL Server для шифрування даних використовуються вбудовані процедури PL/SQL, які послуговуються такими ж алгоритмами, що й у СКБД Oracle (рис. 1).

Проаналізувавши інформаційну систему митних підрозділів, було виявлено, що незаконний доступ до даних може отримати зловмисник під час передання інформації до ЦБД, а також адміністратор БД, який має доступ до незашифрованих даних, що зберігаються в БД. Для захисту даних слід застосувати шифрування. Шифрування даних не розв'язує проблему контролю доступу, однак значно підвищує безпеку збереження даних, адже до них не матимуть доступу всі рівні адміністраторів (рис. 3). Наприклад, якщо сервер центральної бази даних було неправильно налаштовано, і хакер зміг отримати доступ до даних, то вкрадені дані не матимуть ніякої цінності, якщо вони зашифровані.

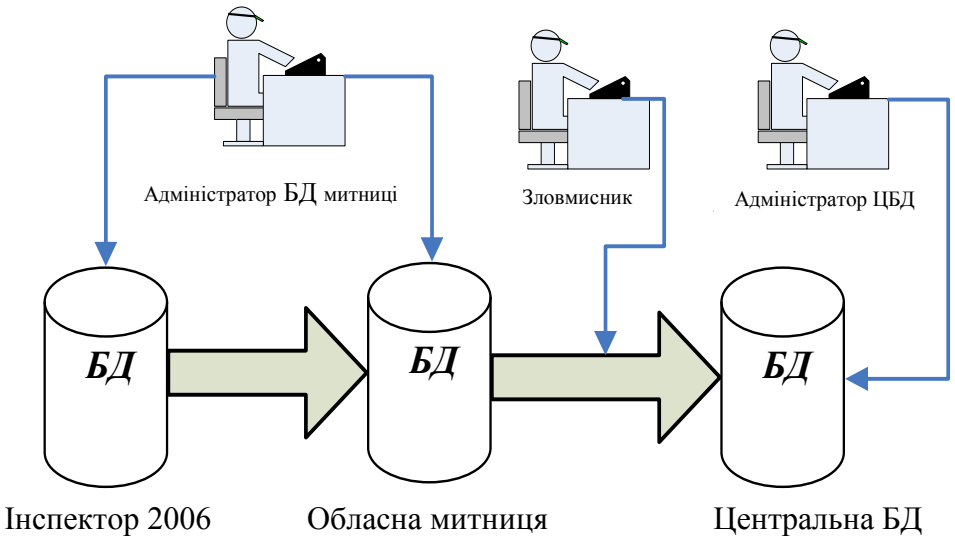


Рис. 1. Перехоплення секретної інформації зловмисником

Хоча шифрування – надійний засіб захисту даних, його не слід застосовувати до всіх даних, тому що під час шифрування суттєво збільшуються обсяг даних і навантаження на процесор сервера. Коли вирішується, чи потрібно шифрувати дані, слід оцінити, чи можуть отримати доступ до комп'ютерної мережі зловмисники. Якщо користувачі отримують доступ до даних через загальнодоступну мережу, для збільшення безпеки може знадобитися шифрування даних. Однак, якщо для доступу передбачено безпечну конфігурацію інтрамережі, шифрування може не знадобитися. Будь-яке використання шифрування також має містити стратегію обслуговування паролів, ключів і сертифікатів.

MS SQL Server дає змогу адміністраторам і розробникам обирати з декількох алгоритмів, зокрема DES, Triple DES, TRIPLE_DES_3KEY, RC2, RC4, RC4 зі 128-розрядним ключем, DESX, AES зі 128-розрядним ключем, AES зі 192-розрядним ключем і AES із 256-розрядним ключем [9].

Якщо для шифрування даних на митних постах використовується MS SQL Server, а в ЦБД Oracle 11g, то потрібно, щоб алгоритми шифрування збігалися. В Oracle 11g асиметричних алгоритмів шифрування немає, їх можна використовувати, якщо придбати утиліту Oracle Advanced Security. В табл. 4 відображено алгоритми шифрування, наявні в Oracle та в MS SQL Server.

Таблиця 4

Алгоритми шифрування, що збігаються

Алгоритм Oracle	Алгоритм MS SQL Server	Довжина ключа, Byte
DES	DES	4
Triple DES	Triple DES	20
3DES_2KEY	3DES_2KEY	14
AES 128	AES 128	8
AES 192	AES 192	12
AES 256	AES 256	16

Щоб виокремити алгоритми, які найдоцільніше використовувати в Єдиній інформаційній системі митної служби, маємо дослідити, як ці алгоритми працюють.

Для проведення порівняльного аналізу запропонованих шифрів розглянемо їхні основні параметри: довжина ключа, кількість раундів шифрування, довжина оброблюваного блоку, який зашифрується, криптостійкість.

Тепер визначимо, скільки часу забере спроба дібрати ключа до алгоритму. Спроба добору ключа розраховується за формулою:

$$T = \frac{p^L}{V \times n},$$

де P – потужність алфавіту ключа, $P = 2$ (0 або 1);

L – довжина ключа;

V – швидкість перенабору на комп'ютері Pentium I 5 із 4 ядрами і тактовою частотою 2,7 GHz – приблизно 2 700 000 000 операцій за секунду, якщо будуть задіяні всі чотири ядра, то швидкість перенабору буде в 4 рази більшою;

n – коефіцієнт переведення, секунд за дні, $n = 3\ 156\ 000$;

Значення розрахованих параметрів для криптоалгоритмів DES, AES подано в табл. 5.

Таблиця 5

Параметри криптостійкості алгоритмів

Алгоритм	Довжина ключа, Bit	Кількість перенаборів для розшифрування	Кількість років для добору ключа
DES	56	2^{56}	2,11
Triple DES	168	2^{168}	$1{,}1*10^{34}$
AES 128	128	2^{128}	$1*10^{22}$
AES 192	192	2^{192}	$1{,}8*10^{41}$
AES 256	256	2^{256}	$3{,}4*10^{64}$

Як бачимо з табл. 5, жоден із алгоритмів неможливо зламати шляхом добору ключа, однак найбільш незахищеними алгоритмами є DES та AES 128. Але й для цих алгоритмів спроба зламати алгоритм шляхом добору ключа забере дуже багато часу.

Для оцінювання швидкодії роботи алгоритмів було розроблено програмний додаток, що працює за певним алгоритмом (рис. 2).

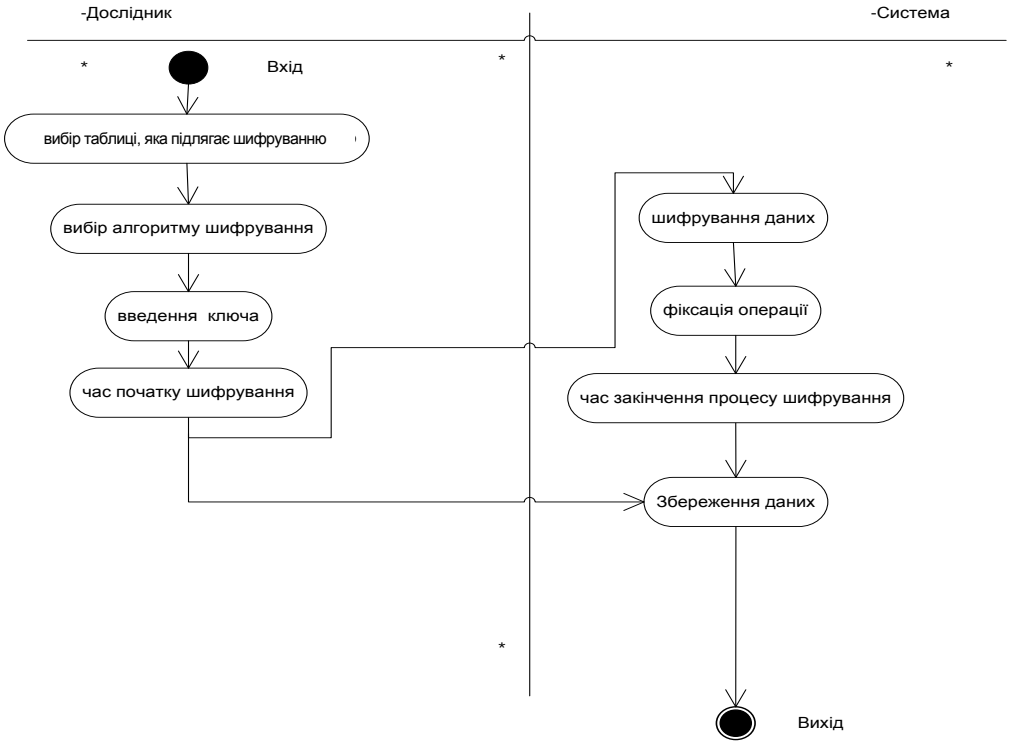


Рис. 2. Алгоритм роботи програмного додатка

Дослідник обирає таблицю, тип алгоритму, який застосовуватиметься для шифрування, потім генерується ключ, далі обирається для шифрування зазначений стовпець із певним типом даних, який потрібно зашифрувати. Під час роботи додатка запам'ятовується t_s – час початку шифрування, t_f – час закінчення шифрування. Різницю між часом початку та закінченням шифрування називаємо швидкодією обраного алгоритму: $T_{cr} = t_s - t_f$. Коли дані буде зашифровано за допомогою вбудованих алгоритмів, експортуємо таблицю, в якій шифрували дані, й оцінюємо, наскільки збільшився розмір таблиці після шифрування.

Для генерації ключів використовується така процедура над вхідними даними, що є довжиною ключа шифрування.

```
CREATE OR REPLACE procedure
 genkey (pl  IN PLS_INTEGER, key out raw)
IS
    BEGIN
    key := dbms_crypto.randombytes (pl);
END genkey;
```

Для генерації ключа застосовується функція `RANDOMBYTES` із пакета `DBMS_CRYPTO`.

Для шифрування даних у СКБД Oracle використовується пакет `DBMS_CRYPTO` з функціями для шифрування даних. Для зручності в роботі з цим пакетом розробляємо функцію шифрування, алгоритм якої зображено на рис. 3. Вхідні дані у функцію – це назва алгоритму шифрування і стовпець із таблиці, який підлягає шифруванню. Оскільки вбудовані в пакет функції шифрування працюють тільки з даними у форматі RAW, то спочатку функція дані зі стовпця перетворює на формат RAW, потім шифрує, після чого перетворює на формат CHAR і перезаписує вже зашифровані дані в таблицю. Функція для розшифрування даних працює аналогічно, тільки замість функції `DBMS_CRYPTO.encrypt` викликається функція `DBMS_CRYPTO.dencrypt` для розшифрування даних (рис. 3).

Для дослідження роботи системи створюємо програмний додаток на мові C#. У проведенні дослідження використовуватимемо таблицю, яка є в демо БД Oracle 11, – це таблиця користувача SH.CUSTOMER, вона має 55 000 записів.

Для шифрування даних обираємо три стовпці `CUST_FIRST_NAME, CUST_LAST_NAME, CUST_STREET_ADDRESS`. Щоб зашифровані дані потім можна було перезаписати в ту саму чарунку таблиці, збільшуємо розмір стовпця до VARCHAR2(4000).

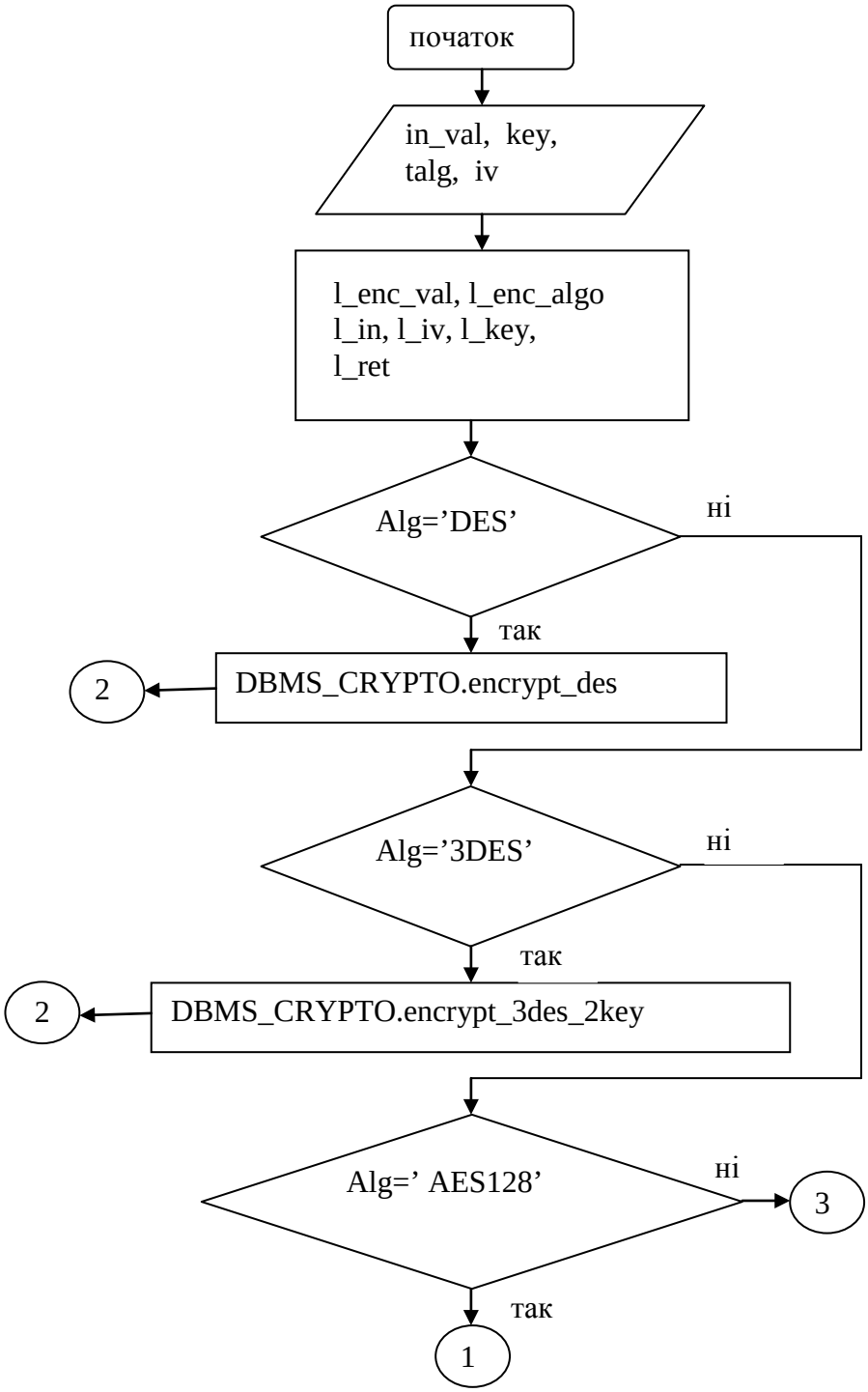


Рис. 3. Алгоритм роботи функції шифрування даних

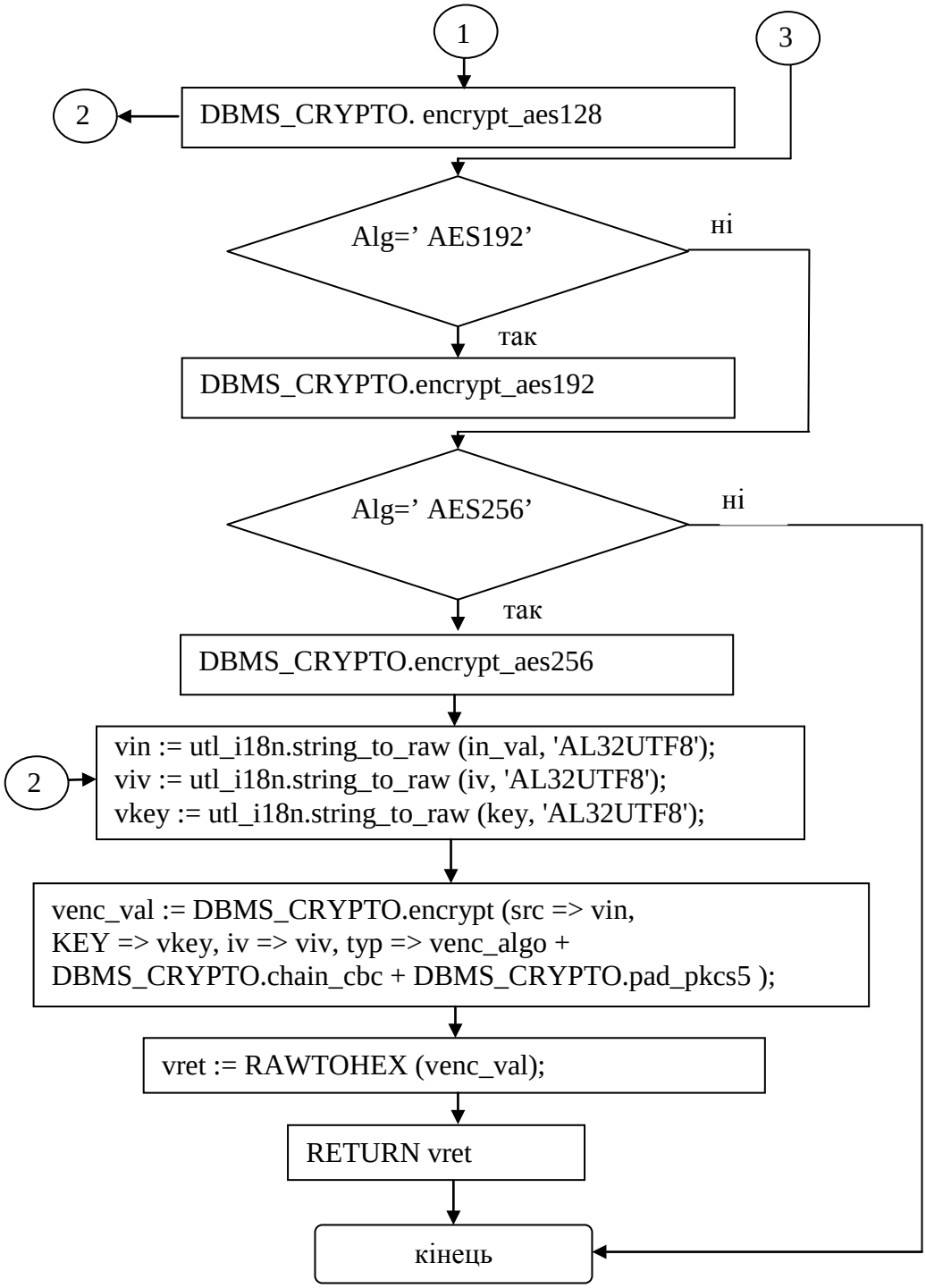


Рис. 3. Алгоритм роботи функції шифрування даних (закінчення)

За допомогою розробленого додатка (рис. 4) зобразимо головне вікно програми.

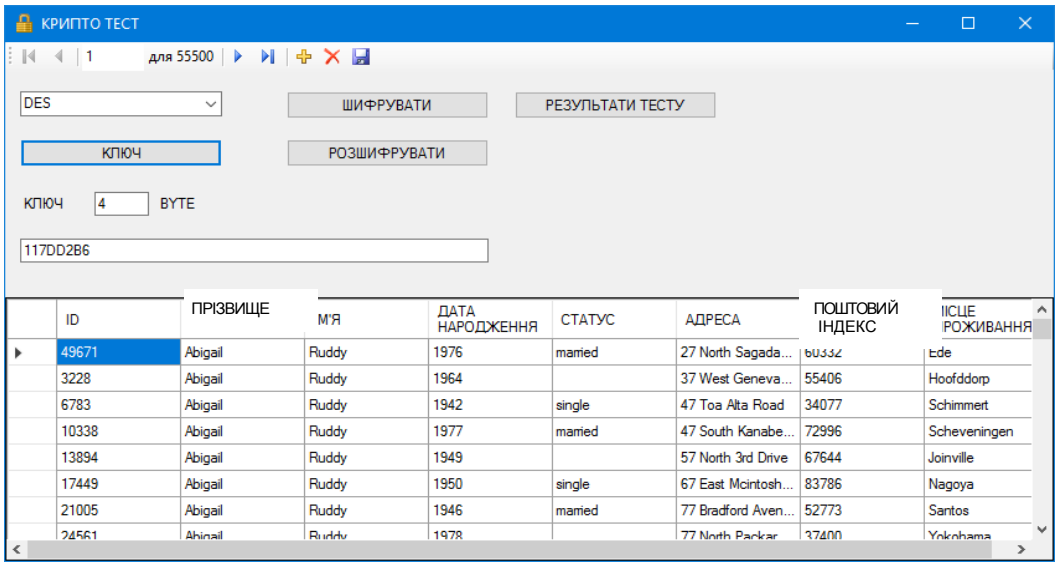


Рис. 4. Головне вікно програми

По черзі обираємо алгоритми шифрування, генеруємо для кожного алгоритму ключ, потім проводимо операції шифрування та розшифрування даних таблиці. Час роботи алгоритмів і розмір файла експорту таблиці заносимо в таблицю “TEST”. Після проведення тестів натискаємо кнопку “Результати тестів”. На рис. 5 зображено результати роботи системи шифрування даних. Час роботи алгоритмів відображається в секундах.

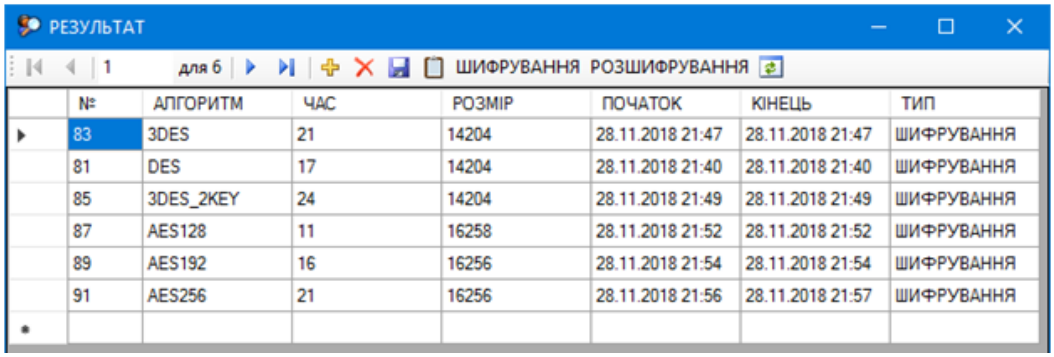
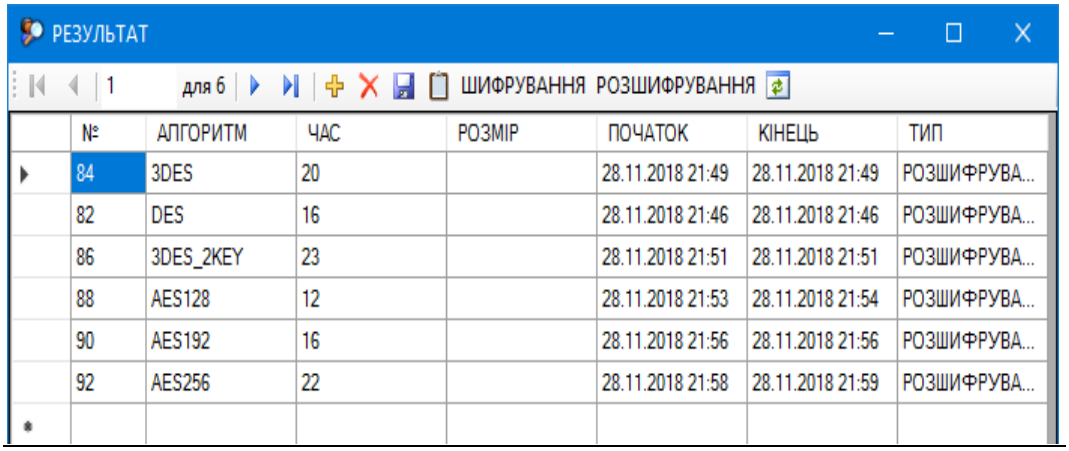


Рис. 5. Результати оцінювання роботи системи в режимі шифрування

Натиснемо на кнопку “РОЗШИФРУВАННЯ”, у вікні “РЕЗУЛЬТАТ” буде виведено дані щодо результату роботи вбудованих алгоритмів у режимі розшифрування даних. На рис. 6 зображено результат роботи системи у режимі розшифрування даних. На рис. 7 – час роботи алгоритмів у вигляді графіка. На рис. 8 відображено залежність розміру зашифрованих даних від режимів шифрування .



№	АЛГОРИТМ	ЧАС	РОЗМІР	ПОЧАТОК	КІНЕЦЬ	ТИП
84	3DES	20		28.11.2018 21:49	28.11.2018 21:49	РОЗШИФРУВА...
82	DES	16		28.11.2018 21:46	28.11.2018 21:46	РОЗШИФРУВА...
86	3DES_2KEY	23		28.11.2018 21:51	28.11.2018 21:51	РОЗШИФРУВА...
88	AES128	12		28.11.2018 21:53	28.11.2018 21:54	РОЗШИФРУВА...
90	AES192	16		28.11.2018 21:56	28.11.2018 21:56	РОЗШИФРУВА...
92	AES256	22		28.11.2018 21:58	28.11.2018 21:59	РОЗШИФРУВА...

Рис. 6. Результат роботи алгоритмів у режимі розшифрування

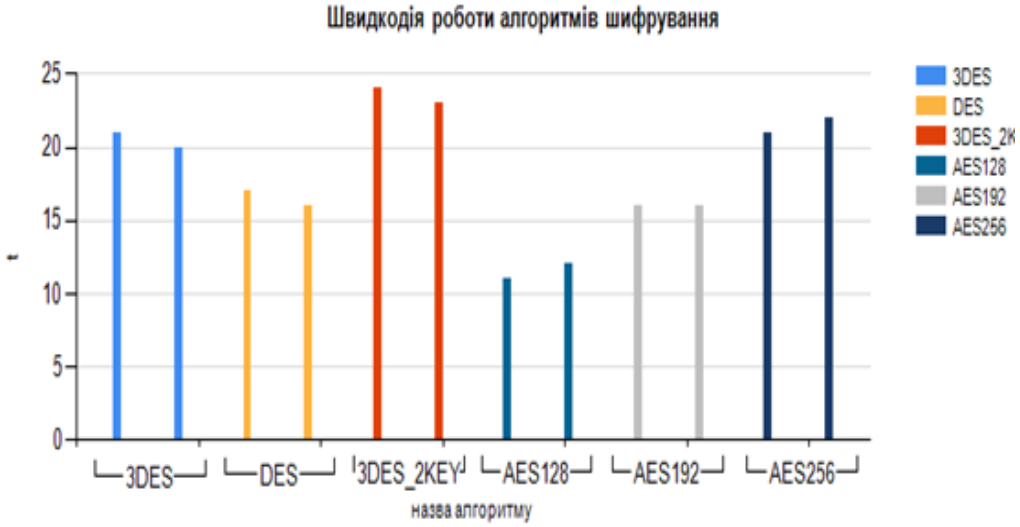


Рис. 7. Результат роботи алгоритмів шифрування у вигляді графіка

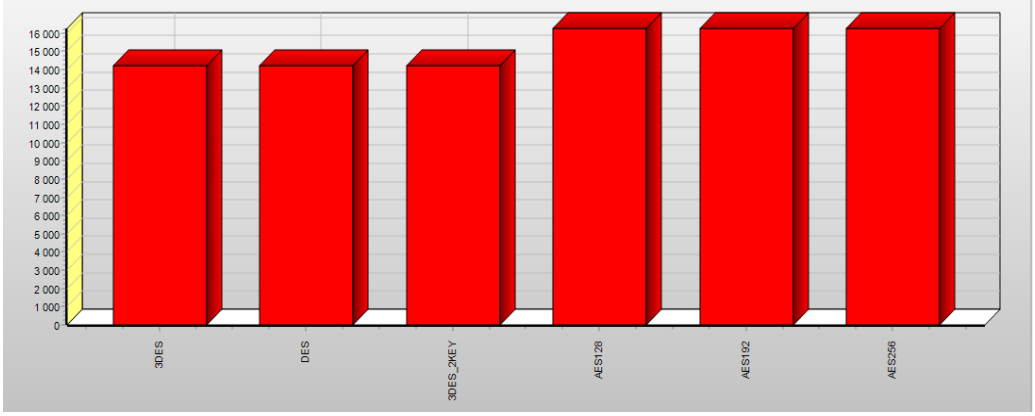


Рис. 8. Залежність обсягу зашифрованих даних від режимів шифрування

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Набув подальшого розвитку метод оцінювання роботи вбудованих симетричних алгоритмів шифрування даних. Запропоновано алгоритм універсальної функції, яка дає змогу шифрувати дані завдяки введеному ключеві та обраному алгоритму. У результаті досліджень роботи вбудованих алгоритмів шифрування отримано такі результати:

1. Найшвидший алгоритм шифрування із вбудованих алгоритмів – AES 128, найповільніший – 3DES_2KEY, але різниця незначна – 5 секунд на 55 500 записів.

2. Під час шифрування даних їхній обсяг збільшується для алгоритмів серії DES удвічі, для алгоритмів AES – утричі.

3. Від довжини ключа залежить швидкодія роботи алгоритму.

4. Обсяг зашифрованих даних не залежить від довжини ключа, він залежить тільки від типу алгоритму (рис. 8).

5. Ресурси, що споживають алгоритми, не залежать ні від довжини ключа, ні від типу алгоритму навантаження на процесор комп'ютера (за всіх видів шифрування – приблизно 30 %).

6. Застосування вбудованих алгоритмів шифрування доцільне лише тоді, коли використовується швидкісна комп'ютерна мережа. Наприклад, в митних підрозділах можливо використовувати цей метод тільки у разі передачі інформації через кручену пару чи оптоволокно. Якщо ми застосуємо цю криптосистему для захисту інформації на митних постах, де використовується супутниковий зв'язок із технологією VSAT, то в пікові години система не зможе передавати збільшений унаслідок шифрування обсяг інформації, це спричинить затори на митниці.

7. Якщо обирати метод шифрування з погляду можливого криптоаналізу та швидкодії, то оптимальним є метод AES 128, він найшвидший.

8. Якщо обирати щодо збільшення обсягу інформації, можливо застосовувати метод 3DES_2KEY. Він хоча й забирає більше часу (як було показано, під час шифрування 55 000 записів спрацював повільніше на 3 с), однак цей метод досить криптостійкий і зашифровані дані збільшуються тільки вдвічі.

Список використаних джерел:

1. *Семенов Ю. А.* Алгоритм DES. URL: http://book.itep.ru/6/des_641.htm
2. *Ходаковський О. С., Літнарович Р. М.* Криптографічний захист інформації. Рівне: МЕГУ, 2012. 108 с.
3. *Mitsuru M.* Linear Cryptanalysis of DES Cipher. URL: https://www.cs.bgu.ac.il/~ beimel/Courses/crypto2001/Matsui.pdf
4. *Ruohonen K.* Mathematical Cryptology. Tampere: Tampere University of Technology, 2010. 136 p.
5. *Daemen J., Rijmen V.* AES – The Advanced Encryption Standard. Berlin: Springer–Verlagm, 2002. 238 p.
6. *Dudykevych V., Bakay O., Lakh Y.* Investigation of Payment Cards Systems Information Security Control // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), (September 12–14, 2013, Berlin, Germany), 2013. P. 651–654. DOI: 10.1109/IDAACS.2013.6663005
7. *Bawna Bhat, Abdul Wahid Ali, Apurva Gupta* DES and AES performance evaluation // International Conference on Computing, Communication & Automation, 15–16 May, 2015. P. 887–890. DOI: 10.1109/CCAA.2015.7148500
8. *Reatrey Pich, Sorawat Chivapreecha, Jaruwit Prabnasak* A single, triple chaotic cryptography using chaos in digital filter and its own comparison to DES and triple DES // 2018 International Workshop on Advanced Image Technology (IWAIT). P. 1–4. DOI:10.1109/IWAIT.2018.8369682
9. *Dilna V., Babu C.* Area optimized and high throughput AES algorithm based on permutation data scramble approach // 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). P. 3056–3060. DOI: 10.1109/ICEEOT.2016.7755263
10. *Akash Kumar Mandal, Chandra Parakash, Archana Tiwari* Performance evaluation of cryptographic algorithms: DES and AES // 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science. P. 1–5. DOI: 10.1109/SCEECS.2012.6184991
11. Using the DBMS_CRYPTO Subprograms. UPL: https://docs.oracle.com/database/121/ARPLS /d_crypto.htm#ARPLS664
12. Choose an Encryption Algorithm. UPL: https://docs.microsoft.com/ru-ru/sql/relational-databases/security/encryption/choose-an-encryption-algorithm?view=sql-server-2017

References:

1 Semenov Yu. A. (2015), *Alhorytm DES* [DES algorithm], available at: http://book. itep.ru/6/des_641.htm [Ukraine].

2 Khodakovs'kyy O. S. and Litnarovych R. M. (2012), *Kryptohrafichnyy zakhyst informatsiyi* [Cryptographic protection of information], Press International Economic-Humanities University, Rivne, 108 p. [Ukraine].

3 Mitsuru M. (1998), Linear Cryptanalysis of DES Cipher, available at: https://www.cs.bgu.ac.il/ ~beimel/Courses/crypto2001/Matsui.pdf

4 Ruohonen K. (2010), Mathematical Cryptology, press Tampere University of Technology, Tampere, 136 p.

5 Daemen J. and Rijmen V. (2002), AES – The Advanced Encryption Standard, Springer–Verlag, Berlin, 238 p. [Germany].

6 Dudykevych V., Bakay O. and Lakh Y. (2013), Investigation of Payment Cards Systems Information Security Control, Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), vol. 2, (September 12–14, Berlin, Germany), pp. 651–654. DOI: 10.1109/IDAACS.2013.6663005 [Germany].

7 Bawna Bhat, Abdul Wahid Ali, Apurva Gupta (2015), DES and AES performance evaluation, International Conference on Computing, Communication & Automation, 15-16 May, pp. 887–890. DOI: 10.1109/CCAA.2015.7148500

8 Reatrey Pich, Sorawat Chivapreecha, Jaruwit Prabnasak (2018), A single, triple chaotic cryptography using chaos in digital filter and its own comparison to DES and triple DES, International Workshop on Advanced Image Technology (IWAIT), pp. 1–4. DOI:10.1109/IWAIT.2018.8369682

9 Dilna V. and Babu C. (2016), Area optimized and high throughput AES algorithm based on permutation data scramble approach, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 3056–3060. DOI: 10.1109/ICEEOT.2016.7755263

10 Akash Kumar Mandal, Chandra Parakash and Archana Tiwari (2012), Performance evaluation of cryptographic algorithms: DES and AES, IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1–5. DOI: 10.1109/SCEECS.2012.6184991

11 Using the DBMS_CRYPTO Subprograms, available at: https://docs.oracle.com/database/121/ARPLS /d_crypto.htm#ARPLS664

12 Choose an Encryption Algorithm, available at: https://docs.microsoft.com/ ru-ru/sql/relational-databases/security/encryption/ choose- an-encryption-algorithm? view=sql-server-2017