ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2010. No. 5(101)*
ELEKTRONIKA IR ELEKTROTECHNIKA

SYSTEM ENGINEERING, COMPUTER TECHNOLOGY
T 120
SISTEMŲ INŽINERIJA, KOMPIUTERINĖS TECHNOLOGIJOS

Power Awareness Experiment for Crypto Service-Based Algorithms

J. Toldinas
Computer Department, Kaunas University of Technology,
Studentų str. 50, LT-51368, Kaunas, Lithuania, e-mail: eugenijus.toldinas@ktu.lt
V. Štuikys, G. Ziberkas
Software Engineering Department, Kaunas University of Technology,
Studentų str. 50, LT-51368, Kaunas, Lithuania, phone: +370 37 300399, e-mail: vytautas.stuikys@ktu.lt, ziber@soften.ktu.lt
D. Naunikas
Computer Department, Kaunas University of Technology,
Studentų str. 50, LT-51368, Kaunas, Lithuania, e-mail: darius.naunikas@stud.ktu.lt

Introduction

As a result of further expansion of Information Communication Technologies (ICT), one can observe the emergence of a new trend in using the technologies now: a global virtualization of the world that is expressed through the term 'cloud computing'. Cloud computing is the future generation of computing which is characterized by main entities - Software, Hardware, Network and ability to use the remote portable resources such as a results of some computations. The collective nature of all these entities, as combined into a coherent system with modern computational features such as mobility, is known as the Cloud [1]. Mobility and mobile computing play a significant role in this context [2]. Because of continued miniaturization, ubiquitous communication, and increasing computation power, mobile handheld (aka Personal Digital Assistant – PDA) users can now perform many online tasks on the go, including web browsing, document editing, multimedia streaming, and Internet banking, to name a few [3].

Though there are many problems yet to be solved within this new computing paradigm, two major concerns should be mentioned in the first place: energy consumption and information security. The first issue is due to an adequate progress of computational power and energy (battery) power (e.g., processor and computer speed have increased thousands times [4], while the battery power is a scarce resource for mobile devices). The second issue is associated with the first one. Indeed, now people want to work on the go, where battery is the main energy resource. Because mobile devices (phones, PDAs, tablet computers, etc.) are as little as possible they simply could be lost or stolen. The information stored in them becomes accessible for the non-authorized use. To reduce such a risk we must encrypt information within the devices.

Security mechanisms address computing services, such as authentication for user admission, intrusion detection and prevention as well as counter-measures for other forms of attacks (e.g., denial of service) and data protection in storage, in e-mails or to provide secure transactions [5].

The aim of this paper is to consider the matching between a family (variants) of the given cryptography algorithms and a given set of prescribed constraints (e.g., performance, energy consumption awareness, safety levels, user profile and various trade-offs amongst the constraints).

The task we consider in the paper is as follows: to identify the energy consumption and performance trade-offs for crypto service that implements four algorithms (DES, 3DES, AES, RC2) within the wide spread technology .NET Compact Framework [6].

Context and general framework to analyze the task

The context of the task is a modern organization (Fig. 1), where a set of battery-dependent mobile devices are connected to the stationary computing resources through wireless communication links. The devices may operate under different operating systems exploited on the go.

Today the technology enables the use of different mobile operating systems as it is depicted in Fig 2. Energy management within operating environments is being performed at multiple layers of the systems: the physical layer, the operating system (OS) layer, and the application layer [7]. Since faster Central Processing Units (CPUs) and larger memories tend to require more power to operate at the same time enabling better

functionality of applications, techniques to reduce and manage energy consumption at the application level are necessary. On the other hand, the application layer should be protected from the malicious interventions of hackers into the systems.

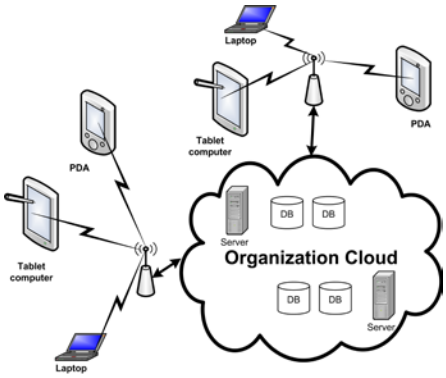


Fig. 1. Modern organization structure based on cloud computing

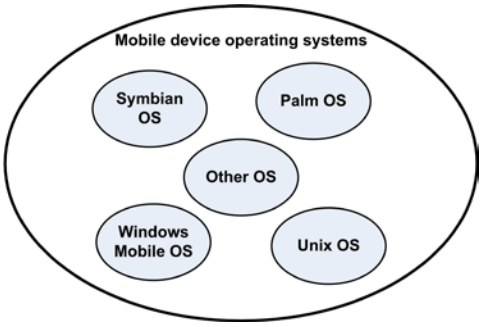


Fig. 2. Mobile device operating systems

Providers of mobile devices and their software try to solve the security issues proposing different approaches such as anti-virus or file encrypt-based. One way for file encryption is the operating system tool, such as bit locker, or the encryption with well-known cryptographic algorithms. The other solution to security proposes a Security Content layer as Anti-virus and File Encrypt facilities.

Microsoft ® proposes a Modern .NET framework technology that has the crypto service provider (Fig.3) with service providers for information encryption/decryption on handheld PC with DES, 3DES, AES, RC2 algorithms [6].

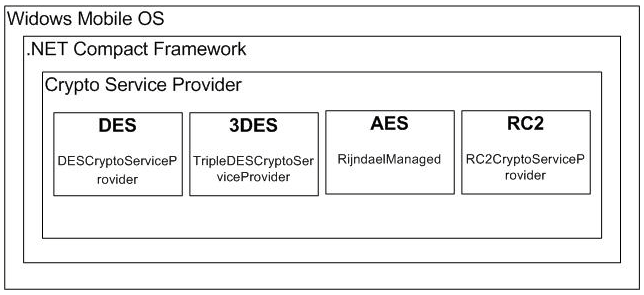


Fig. 3. .NET Compact Framework Crypto Service Provider based on [6]

When we have the crypto service provider with well known algorithms, we can use it for information encryption/decryption. However, the information hiding comes not for free: that requires energy resources, too. As it has been already mentioned, awareness of the energy consumption is highly important in mobile devices. But how we can ensure the needed functionality, the reasonable use of energy and the different information security levels at the same time? What is trade-offs of those contrasting requirements? Empirically we can predict that stronger cryptography algorithms consume more energy. In such a way 3DES must consume more energy than DES, because it repeats the DES cryptography three times. Thus there are many unclear questions we try to give an answer through some experiments we describe in this paper.

In Fig. 4, we present a general scheme that is to be connected with the .NET Compact framework (Fig. 3) to provide our experiments. We have selected two types of information (documents and pictures) to be encrypted and decrypted as the most relevant of applications.

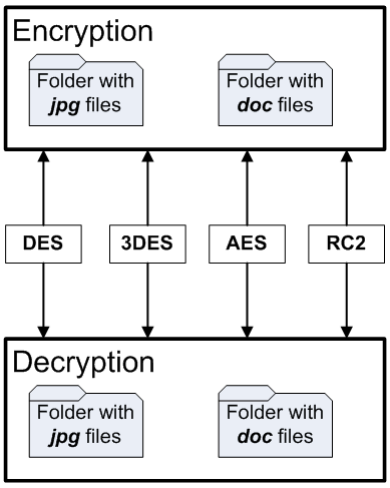


Fig. 4. Cryptography algorithms and file types

Note that here we try to protect information files (e.g., documents, secure personal information, etc.), but not the program files which constitute a separate security problem.

Methodology

The task of the experiments is to identify various dependencies among the energy consumption features, encryption/decryption modes, different cryptography algorithms and different information types. Fig. 5 outlines an algorithm that enables to perform measurements of energy consumption and obtain the desired relationships. We apply the OS-based measuring scheme [9], where the amount of the consumed energy over time is periodically written to the file during the data cryptography process.

The energy consumption values for individual cryptographic algorithms are obtained by running their .NET Compact Framework Crypto Service Provider implementations, and measuring the current battery drawn. For getting valuable results of battery drain when data is encrypted/decrypted, we iterate cryptography process. Because encryption and decryption time may vary we perform encryption and decryption separately.

Before starting cryptography process we identify: the number of iterations (**NI**), the cryptography algorithm (**DES, 3DES, AES, RC2**), and the cryptography direction

(**ED** - encryption or decryption). To ensure a more precise measurement results we eliminate some energy consumption features such as display backlight and graphic card by turning it off before starting cryptography process (Fig. 5). Selected files for encryption/decryption were used separately: documents (**doc** format) and pictures (**jpg** format).

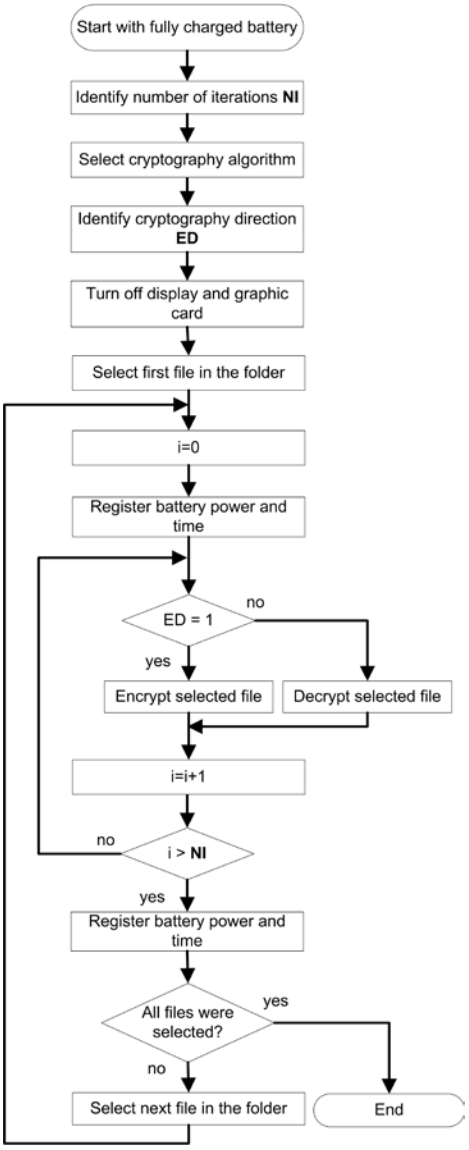


Fig. 5. Energy measurement algorithm for a given crypto algorithm

The algorithm exploits the only one crypto algorithm at a time starting with the fully charged battery (100%). Next what is important to note is that we need to allow discharging the battery until approximately 20%. To achieve this level when operating we need to manage the process as flexibly as possible because there are severe restrictions on memory size and availability to obtain the measured values. For this purpose, we have applied the cryptography for two types of files (document and picture) within created folders DOC and JPG, and placed there the appropriate files of the different length (the type of folder is not specified in Fig. 5). We use own files because benchmark files were not found for our context. The size of the files in folders is limited by the size of random-access memory (RAM). Files placed in the folders were selected to achieve approximately the same size of the DOC folder (6,87MB) and the JPG folder (6,86MB). Files were sorted in descending order by the file size because we did iterations of cryptography algorithm to reach suitable measurement results, and files with bigger size were first encrypted/decrypted through the iterations. The iteration number NI we have identified experimentally (e.g., for DES NI=1500, for 3DES NI=1000, for AES NI=200 and for RC2 NI=100).

Experiments

To realize the experiments we have developed the program that implements the algorithm (Fig. 5) in C# language for .NET Compact Framework. The experiments were performed on the PDA of the model ASUS P750 (Pocket PC platform, Intel PXA270 520 MHz CPU, 256 MB RAM, Windows Mobile © 6 Professional CE OS 5.2). We used .NET Compact Framework 3.5 version. The DOC folder contains nine files sorted in descending order by file size (9.doc-1.825KB, 8.doc-1.593KB, 7.doc-1.055KB, 6.doc-803KB, 5.doc-593KB, 4.doc-421KB, 3.doc-340KB, 2.doc-286KB, 1.doc-124KB). The JPG folder contains seven file sorted in descending order by the file size (7.jpg-1.871KB, 6.jpg-1.664KB, 5.jpg-1.285KB, 4.jpg-918KB, 3.jpg-619KB, 2.jpg-450KB, 1.jpg-229KB).

We provide the summary of the experiment results in Tables 1 (for .doc files) and Table 2 (for .jpg files). Each Table contains the crypto algorithms, the amount of encrypted/decrypted information in MB, elapsed time and total consumed energy in % for that amount of information. For example, in order to encrypt about 10GB using the DES algorithm computer needs about 6 hours of processor's time and consumes about 80% of energy.

Table 1. Summary of the experimental results (document files encryption-decryption)

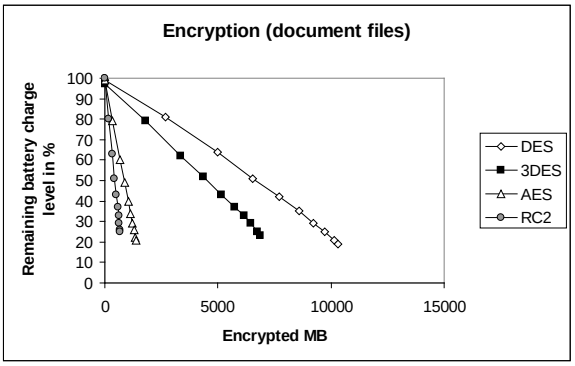
Encryption			
Crypto algorithm	Amount of information MB	Elapsed time hh:mm	Battery power consumed %
DES	10308	06:19	80
3DES	6873	05:39	74
AES	1374	05:58	78
RC2	687	06:32	75
Decryption			
Crypto algorithm	Amount of information MB	Elapsed time hh:mm	Battery power consumed %
DES	550	06:51	79
3DES	482	06:06	72
AES	962	04:58	64
RC2	550	07:10	84

Note. In the second column of Table 1, the amount of information is calculated according to the number of iterations NI (see values at the end of the previous section).

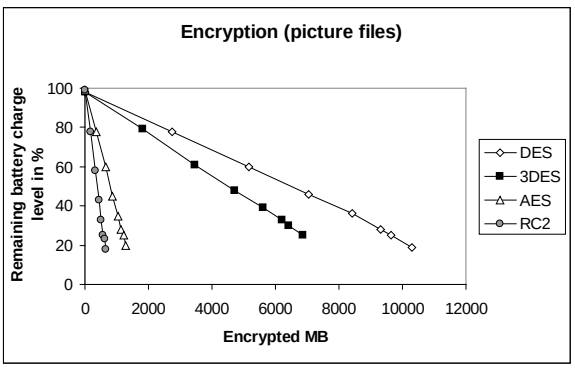
Table 2. Summary of the experimental results (picture files encryption-decryption)

Encryption			
Crypto algorithm	Amount of information MB	Elapsed time hh:mm	Battery power consumed %
DES	10301	06:01	79
3DES	6868	05:35	73
AES	1294	06:08	79
RC2	647	07:15	81
Decryption			
Crypto algorithm	Amount of information MB	Elapsed time hh:mm	Battery power consumed %
DES	549	06:38	77
3DES	482	06:30	75
AES	961	04:52	63
RC2	518	07:21	83

As Tables 1 and 2 provide us with the final measurement points only, we deliver the details of the process in charts. In Fig. 6, we present all measured points for each algorithm when document files (a) and picture files (b) are encrypted. In Fig. 7, we present all measured points for each algorithm when document files (a) and picture files (b) are decrypted. We can see that either encryption or decryption for document files and picture files consume approximately the same amount of energy (if they are about of the same size). Next, the energy consumption either in encryption or decryption mode linearly depends on the file size.

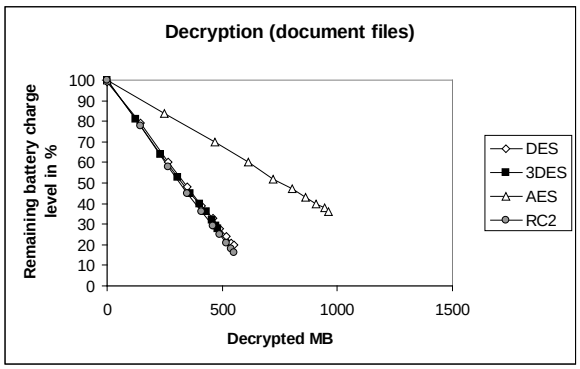


a)

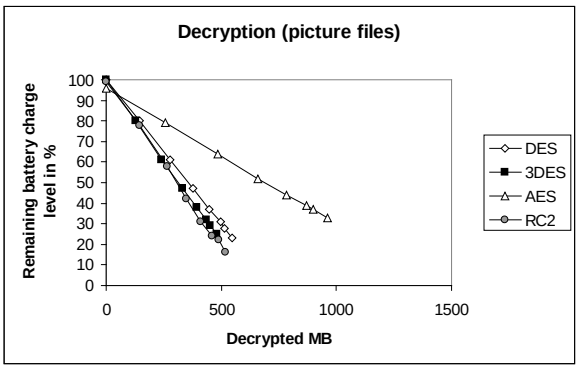


b)

Fig. 6. Energy consumption when encrypted document files (a) and picture files (b)



a)



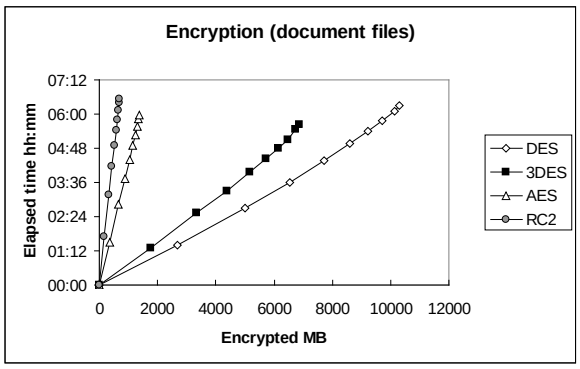
b)

Fig. 7. Energy consumption when decrypted document files (a) and picture files (b)

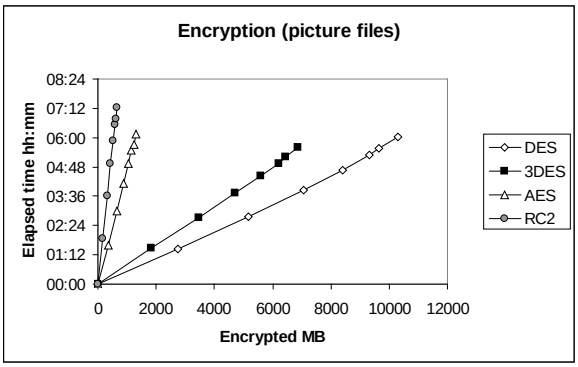
In Fig. 8 and 9, we deliver time-information amount dependencies for the same encryption/decryption algorithms and files used. Again, there is a linear dependency among those factors.

Now let us compare the behavior of encryption and decryption algorithms with respect to energy consumption. As we can see (cp. Fig. 6 and Fig. 7) that decryption requires much more battery energy and time resources than encryption for algorithms DES and 3DES. However, the remaining algorithms behave in other manner.

We explain those discrepancies in detail in Fig. 10. For getting more visible results, we calculate battery energy consumption for the 100MB of encrypted/decrypted information by each type of crypto algorithms (Fig. 10).

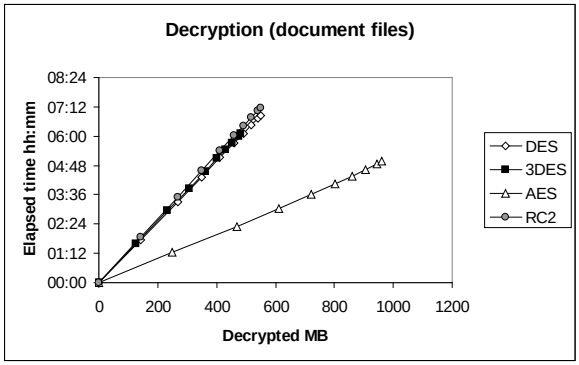


a)

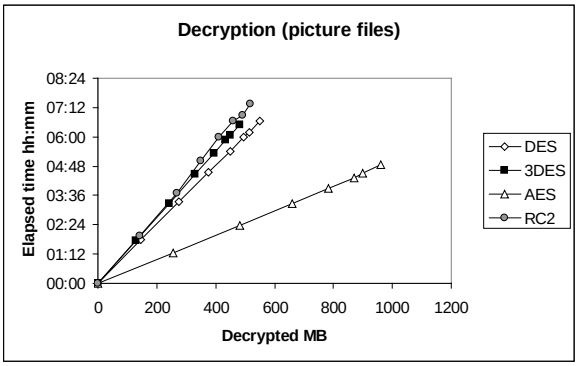


b)

Fig. 8. Time consumed when encrypted document files (a) and picture files (b)

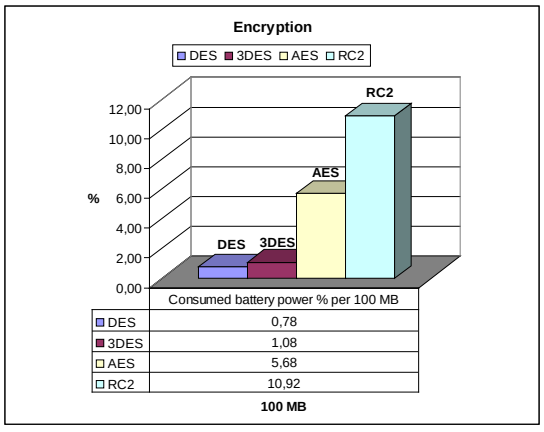


a)

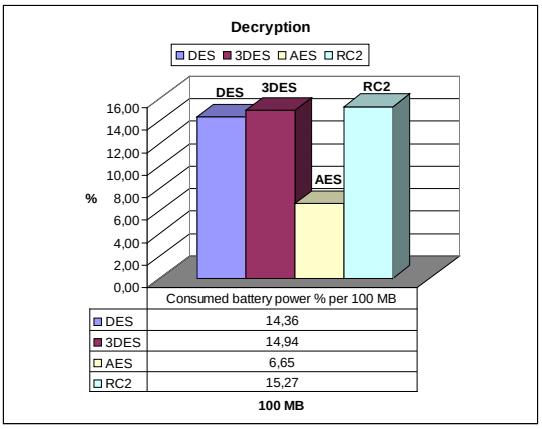


b)

Fig. 9. Time consumed when decrypted document files (a) and picture files (b)



a)



b)

Fig. 10. Battery energy consumption by crypto algorithms for encryption (a) and decryption (b) of 100 MB of information

Note. also that prior of using an algorithm a length of the encryption key is to be selected first and then generated its value. In all experiments we depicted in Charts and Tables the key length was as follows: 4 blocks x 16 bytes for DES and 128 bytes for AES and RC2.

Discussion, evaluation and conclusions

We have selected for our energy-based experiments the Microsoft .NET Compact Framework as a modern and widely used platform for the safe mobile program development and secure information management. Though there are a wide variety of encryption/decryption algorithms we were restricted with the four algorithms used within the Framework. The behaviour of different encryption algorithms with respect to energy consumption is highly different: for the same amount of information (100 MB), e.g., RC2 requires approximately twice more energy than AES and about twelve times more than 3DES. Encryption and decryption modes of AES and RC2 require approximately the same amount of energy for the same information. However the modes of the first algorithms (DES and 3DES) behave quite differently: the decryption mode requires about fifteen times more energy.

In a wider context, from a user perspective, one could interpret the presented results in the following way. There is a great deal of variability of using the results. The basic variable features, as related to the energy consumption, are:

- algorithm class (symmetric, asymmetric, encryption, decryption);
- algorithm type (for our case DES, 3DES, AES, RC2);
- block size (for DES, 3DES), and length of key (128, 192**, 256**, for AES and RC2; ** - are not implemented in the Framework we have used);
- information type a user needs to manage (secret, unsecured);
- the amount of the information for each type;
- mode of the information is to be managed (no use of the algorithms, decryption and the use of a particular part of information, decryption-use-encryption, use-encryption).

Having the results, such as ones in Fig. 10, knowing the needs for the information safety levels, the amount of information to be protected and current state of the battery, a user can reasonably decide of how the task is to be managed with the energy savings in mind.

However, the better strategy is to develop a program that using the collected data would give the prediction and advice on energy/safety trade-offs for a user depending on his/her profile.

References

1. **Pokharel M., Park J.** Cloud computing: future solution for e-governance // Proc. of the 3rd International Conference on Theory and Practice of Electronic Governance. – Bogota, Columbia, November 10–13, 2009. – P. 409–410.
2. Gartner. Gartner News Room, January 18, 2010. http://www.gartner.com/it/page.jsp?id=1282413.
3. **Kim H., Smith J., Shin K.** Detecting Energy–Greedy Anomalies and Mobile Malware Variants // Proc. of MobiSys'08. – Breckenridge, Colorado, USA, June 17–20, 2008. – P. 239–252.
4. **Garret M.** Powering down // Communication of the ACM. – New York: ACM media, 2009. – Vol. 51. – No. 9. – P. 43–46.
5. **Venugopalan R., Ganesan P., Peddabachagari P.** Encryption Overhead in Embedded Systems and Sensor Network Nodes: Modeling and Analysis // Proc. of CASES'03. – San Jose, California, USA, 2003. – P. 188–197.
6. Microsoft Corporation, .NET Framework Developer Center. http://msdn.microsoft.com/en–us/netframework/default.aspx
7. **Toldinas E., Štuikys V., Damaševičius R., Ziberkas G.** Application–Level Energy Consumption In Communication Models For Handhelds // Electronics and Electrical Engineering. – Kaunas: Technologija, 2009. – No. 6(94). – P. 73–76.
8. **Raghunathan A., Ravi S., Hattangady S., Quisquater J–J.** Securing Mobile Appliances: New Challenges for the System Designer // Proc. of the 3d IEEE Int. Conf. on Design, Automation and Test in Europe (DATE'03), IEEE 2003.
9. **Damaševičius R., Štuikys V., Toldinas E.** Embedded program specialization for multiple criteria trade–offs // Electronics and Electrical Engineering. – Kaunas: Technologija, 2008. – No. 8(88). – P. 9–14.

Received 2010 03 22

J. Toldinas, V. Štuikys, G. Ziberkas, D. Naunikas. Power Awareness Experiment for Crypto Service-Based Algorithms // Electronics and Electrical Engineering. – Kaunas: Technologija, 2010. – No. 5(101). – P. 57–62.

In the context of cloud computing two interrelated problems (awareness of power consumption and information safety of mobile devices) are highly important issues. The paper presents some results of experiments we have carried with 4 standard cryptography-based algorithms (AES, RC2, DES and 3DES) aiming to identify their greediness for energy, as well as to collect data for identification of relationships among various characteristics (folder size, information type, security level, algorithm type, encryption/decryption mode, performance/energy, etc.). The experiment is based on our previously developed methodology. The basic results are: 1) performance/energy characteristics are linearly dependent on the folder size and practically independent upon the information type (document or picture), 2) decryption requires much more energy resources then encryption for some class of algorithms. Ill. 10, bibl. 9, tabl. 2 (in English; abstracts in English, Russian and Lithuanian).

Е. Толдинас, В. Штуйкис, Г. Зиберкас, Д. Науникас. Эксперимент определения потребляемой энергии алгоритмами на базе крипто-сервиса // Электроника и электротехника. – Каунас: Технология, 2010. – № 5(101). – С. 57–62.

В контексте распределенных вычислительных ресурсов две взаимозависимые проблемы (понимание процесса потребления энергии и безопасность хранения информации в мобильных устройствах) имеют особое значение. В статье представлены результаты эксперимента, проведенного нами с 4-мя алгоритмами шифрования данных (AES, RC2, DES and 3DES) с целью определения их энергоемкости, а также сбора данных для идентификации взаимозависимости между различными характеристиками (размер каталога, тип информации, уровень безопасности, тип алгоритма, режим шифрования/дешифрования, быстродействие/энергопотребление и т.д.). Эксперимент основан на ранее разработанной нами методологии. Основные результаты: 1) характеристики быстродействия/энергопотребления линейно зависимы от размера каталога и практически независимы от типа информации (текст или графика), 2) в отличие от шифрования, дешифрование требует больших ресурсов энергии для некоторых алгоритмов. Ил. 10, библ. 9, табл. 2 (на английском языке; рефераты на английском, русском и литовском яз.).

J. Toldinas, V. Štuikys, G. Ziberkas, D. Naunikas. Energijos suvartojimo kriptografijos paslaugos algoritmams eksperimentas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2010. – Nr. 5(101). – P. 57–62.

Virtualizacijos ir mobilumo kontekste didelę reikšmę turi dvi tarpusavyje susijusios problemos: energijos vartojimo supratimas ir informacijos apsauga mobiliuosiuose įtaisuose. Šiame straipsnyje pateikiami kai kurie eksperimento su keturiais standartiniais kriptografijos algoritmais (DES, 3DES, AES, RC2) rezultatai, siekiant nustatyti jų energijos imlumą, taip pat surinkti duomenis, kad būtų galima rasti įvairių charakteristikų (katalogo dydžio, informacijos tipo, saugumo laipsnio, algoritmo tipo, užšifravimo ir iššifravimo elgsenos, našumo ir laiko bei energijos) tarpusavio priklausomybes. Eksperimentas atliktas pagal anksčiau pasiūlytą metodiką. Pagrindiniai rezultatai tokie: 1) našumo ir energijos charakteristikos yra tiesiškai priklausomos nuo katalogo, kurį reikia užšifruoti ir iššifruoti, dydžio ir praktiškai nepriklauso nuo informacijos tipo (tekstas ar paveikslas); 2) kai kuriems algoritmams (DES ir 3DES) iššifruoti reikia daugiau energijos (net 15 kartų) negu užšifruoti. Il. 10, bibl. 9, lent. 2 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).

DOI: 10.5755/j02.eie.9426