An Android mobile RC4 simulation for education

Etika Kartikadarma†, Tri Listyorini‡ & Robbi Rahim*

Universitas Dian Nuswantoro, Semarang, Indonesia†
Universitas Muria Kudus, Kudus, Indonesia‡
Universiti Malaysia Perlis, Kubang Gajah, Malaysia*

ABSTRACT: Technological developments affect society lifestyles in various ways; for example, students and lecturers commonly have Android-based mobile phones, but do not make maximum use of them. An Android-based RC4 cryptographic algorithm simulation application was developed for educational purposes in a university setting. This development increases the benefits of an Android-based device by helping students to learn. Based on analysis of the results, it was concluded that the developed RC4 simulation application has met the criteria of validity, effectiveness and practicality.

INTRODUCTION

Cryptography [1-4] uses encryption and decryption to secure data, so that it cannot be easily read. There are many classical and modern algorithms that can be used to secure data, such as the Caesar cipher; Vigenère cipher, one-time pad (OTP); data-encryption standard (DES); GOST (a set of technical standards) [5]; modular multiplication-based block cipher (MMB) [4]; advanced encryption standard (AES); RSA algorithm (Rivest, Shamir and Adelman, who invented the process); RC4 (a stream cipher), RC5 and RC6. The fundamental difference between classical and modern algorithms is that modern algorithms require mathematical processes for encryption and decryption [5-9].

The RC4 is an algorithm that is used widely [8-11]. Students and lecturers new to cryptography find RC4 difficult due to the mathematical content of the RC4 algorithm [8][12]. To facilitate knowledge of the RC4 algorithm, an RC4 Android-based mobile simulation has been created that can be easily accessed.

The RC4 simulation shows in detail the computation of the RC4 algorithm and the encryption and decryption process, such as Blum Blum Shub (BBS), a pseudorandom number generator for key scheduling optimisation [13]; Rabin-Miller as the prime number generator [14] and, permutation and rotation of the encryption and decryption process. Implementing the mobile-based RC4 learning algorithm is expected to help students or even lecturers to learn cryptography more easily by following the simulation of the RC4 algorithmic procedures.

METHODOLOGY

Rivest code 4 (RC4) is a symmetric key and stream chipper cryptography algorithm created by RSA Data Security Inc (RSADSI) [12], by using keys 1 to 256 bytes key function to initialise 256 bytes of tables to use as initiation pseudo random and XOR with plaintext to produce ciphertext and also *vice versa* [8]. The RC4 algorithm uses two arrays consisting a key array (K) that contains key element based on variable length.

The second array, array state (S), is a 256-long array containing permutations from 0 to 255. The RC4 algorithm is based on the above explanation of the array K initialisation with key repeated until it satisfies array K[0], K[1], ..., K[255] is completely filled. Furthermore, the initialisation of array S starts from S[0] to S[255]:

for i = 0 to 255 K [i] = Lock [i mod keylog]
S-Box initialisation process (Array S):
for i = 0 to 255 S [i] = i

Then, do the S-box randomisation step with the following steps:

i = 0; j = 0
for i = 0 to 255 {
j = (j + S [i] + K [i]) mod 256
swap S [i] and S [j] }

After that, create a pseudo random byte with the following steps:

i = (i + 1) mod 256
j = (j + S [i]) mod 256
swap S [i] and S [j]
t = (S [i] + S [j]) mod 256
K = S [t]

Byte K is XOR with plaintext to generate ciphertext or XOR with ciphertext to generate plaintext. This encryption is very fast about 10 times faster than DES and the result much better than few algorithms like DES [8].

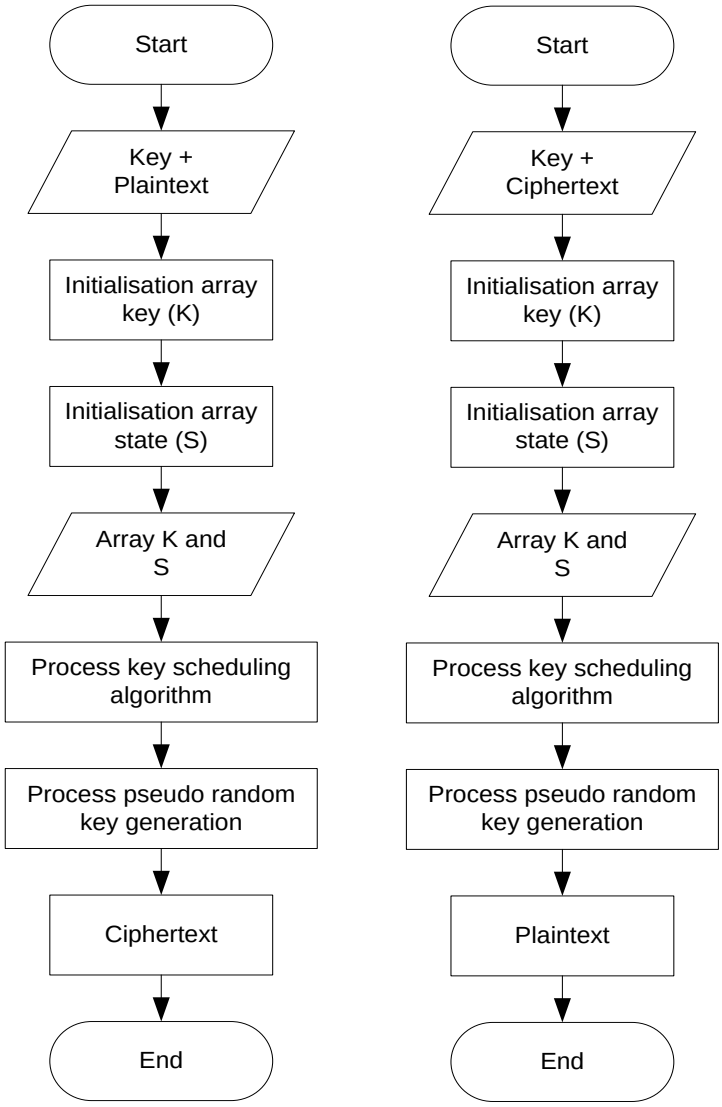

Figure 1: Encryption process (left), decryption process (right).

Mobile Learning

The function of media in learning is to create a more meaningful, quality learning outcome [15][16]. In recent times, the use of mobile devices has increased to the point where almost all students and lecturers have smartphones. However, smartphones are generally used only for short message services (SMS), phone calls, chats, Internet access and entertainment, such as games and music [15][16].

On the other hand, the use of mobile devices in the world of education in general and cryptographic learning in particular is still minimal [15].

The growing number of people who have mobile devices opens the possibility of using mobile technology devices in education. The use of mobile devices in the learning process is known as mobile learning or m-learning. With m-learning the learner can learn anytime and anywhere by using mobile device technology.

The presence of m-learning will not replace electronic learning (e-learning), which is commonly used or replace face-to-face learning in the classroom. The presence of m-learning is intended as a complement to existing learning and provides an opportunity for students to re-learn material whenever and wherever they wish.

This can provide a new and different learning experience for students.

In this article is discussed an Android application that was developed by the authors as a medium of cryptographic learning, specifically for the learning of RC4 algorithm cryptography.

RESULTS AND DISCUSSION

The Android application contains RC4 cryptographic material and can be operated on Android devices or a Windows-based computer or laptop. The minimum requirements to run this application on an Android device are:

1. ARMv7 processor with vector FPU, minimum 550MHz, OpenGL ES 2.0, H.264 and AAC HW decoders;
2. Minimum Android 4.0;
3. Android studio 1.x;
4. RAM 512 MB.

The minimum requirements to run this application on a computer or laptop with the Windows operating system are:

1. 2.33 GHz or faster x86-compatible processor or Intel Atom TM 1.6G Hz or faster processor for netbook devices;
2. Microsoft® Windows® XP, Windows 7 Ultimate (including 64-bit editions) and Windows 10;
3. 1 GB of RAM (recommended 2 GB).

Figures 2, 3 and 4 show a learning simulation of the RC4 algorithm. The RC4 algorithm process is shown gradually starting from plaintext to key, KSA (key-scheduling algorithm) formation, PRGA (psuedo random generation algorithm) and finally encryption/decryption.

An experiment was performed using an Android 4.0 emulator from Android Studio. All functions ran successfully without error in the simulation.

Trials conducted on students and lecturers using the mobile-based RC4 algorithm simulation elicited positive responses, with the learning easy to follow. This application allows plaintext and the key to be inputted manually to the KSA and PRGA processes. Hence, students and lecturers can experiment with various plaintext and keys.

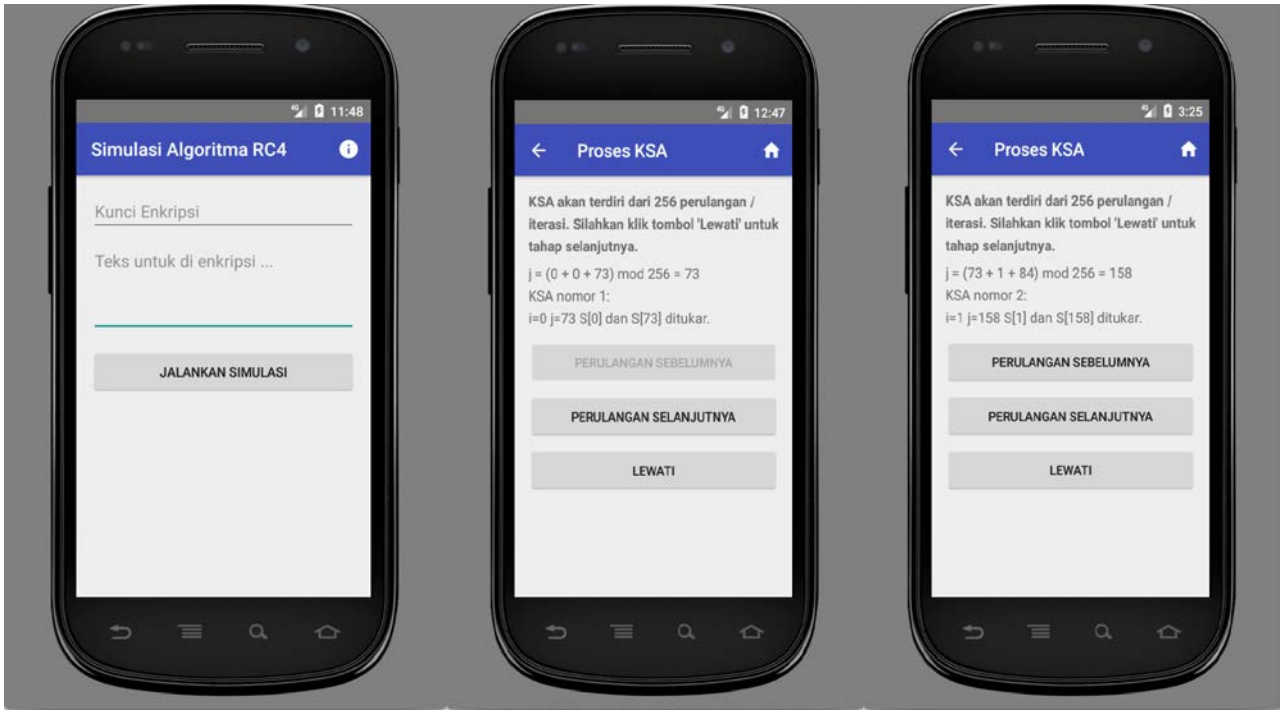

Figure 2: Main display and key-scheduling algorithm (KSA).

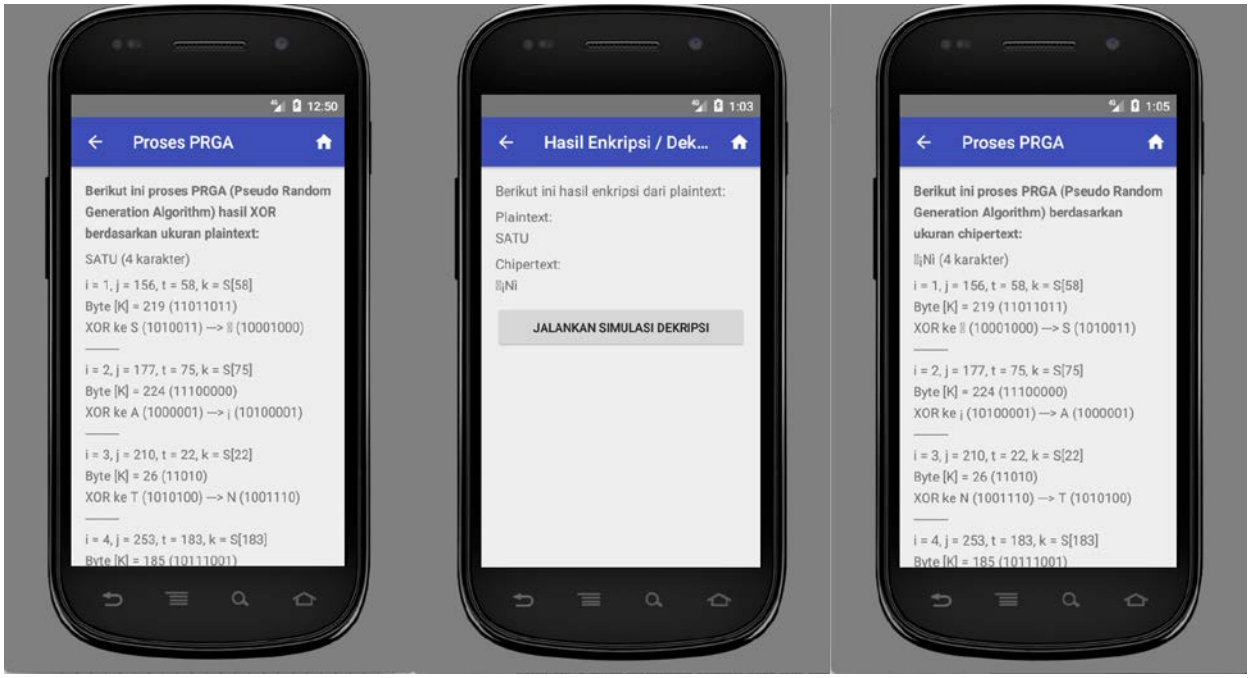

Figure 3: Pseudo random generation algorithm (PRGA) and encryption/decryption process.

IMPACT ON ENGINEERING AND TECHNOLOGY EDUCATION

In the application there are *simulation, evaluation and glossary* menus. Simulation contains the RC4 cryptographic algorithm to demonstrate encryption and decryption. After covering the simulation, the user can test their knowledge of cryptography through the evaluation menu. The last menu, glossary, contains terms related to RC4 cryptography.

Based on the results of experiments, it was concluded that it is feasible to use the learning media application developed by the authors. The RC4 simulation application described in this article can run only on Android (4.0 minimum) mobile devices. It is expected that similar applications will be developed to run on other devices with different versions of Android. The development of learning applications for mobile devices should increase the benefits of mobile devices in the field of education.

The next step, after the application was completed, was to validate its use by students and lecturers on computer security courses. Trials were conducted to validate the practicality and feasibility of the application. Thirty students were selected, all of whom had Android devices or laptops with the Windows operating system. Based on the results of the validation, the lecturers obtained positive percentages from students, of 81.52% and 83.49%. Based on these results, the developed media can be considered practical, and hence feasible to use. Comments and suggestions from lecturers are shown in Table 1. Comments and suggestions from students are shown in Table 2.

Table 1: Comments and suggestions by lecturers.

Validator	Suggestion
Lecturers	For evaluation, it would be nice if it was equipped with a key answer, so that if students answer wrongly, they know the correct answer for the given problem.

Table 2: Comments and suggestions by students.

No.	Suggestions and comments
1.	More animations would be more interesting.
2.	Learning using the Android application is very effective and interesting.
3.	It should be made like a game so as to be more interesting, fun and exciting.
4.	The program is good, but would be more interesting, if the font was replaced with funny forms and an animated cartoon.
5.	The animation is pretty smooth. However, trying to make an application like this with different material may be difficult.

The assessment by lecturers and students was that the application was *very good*. Based on the assessment results it can be concluded that the developed learning media meet validity and qualification requirements.

CONCLUSIONS

The Android-based RC4 algorithm simulation application was successfully developed and has had positive results in teaching and learning. Any instructional material can be delivered by a mobile, which enables another form of learning other than face-to-face. The use of an Android smartphone as a medium of learning is very appropriate, since almost everyone has and needs a smartphone; so why not use it for learning.

The simulation application described here is far from perfect and needs further development to provide more benefits to students and lecturers. Development may include adding further algorithms, especially classic algorithms. These are easy to implement, because they do not need many mathematical formulae. Algorithms that could be implemented include MMB, GOST, IDEA (international data encryption algorithm), DES, Triple DES (3DES), AES, and also RSA. Also there is a need to create a question/answer form for simulation questions and problems.

REFERENCES

1. Rahim, R., Dahria, M., Syahril, M. and Anwar, B., Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression. *World Trans. on Engng. and Technol. Educ.*, 15, **3**, 292–297 (2017).
2. Rahim, R., Man-in-the-middle-attack prevention using interlock protocol method. *ARPN J. of Engng. and Applied Sciences*, 12, **22**, 6483-6487 (2017).
3. Nurdiyanto, H., Rahim, R. and Wulan, N., Symmetric stream cipher using triple transposition key method and Base64 algorithm for security improvement. *J. of Physics: Conf. Series*, 930, **1**, 12005 (2017).
4. Nurdiyanto, H. and Rahim, R., Enhanced pixel value differencing steganography with government standard algorithm. *Proc. 2017 3rd Inter. Conf. on Science in Infor. Technol.*, 366-371 (2017).
5. Attaran, M. and VanLaar, I., Privacy and security on the Internet: how to secure your personal information and company data. *Infor. Manage. & Computer Security*, 7, **5**, 241-247 (1999).
6. Schneier, B., Applied Cryptography (1996).
7. Mollin, R.A., *An Introduction to Cryptography*. Chapman & Hall/CRC (2007).
8. Jindal, P. and Singh, B., RC4 encryption - a literature survey. *Procedia Computer Science*, 46, 697-705 (2015).
9. Jian, X. and Xiaozhong, P., An improved RC4 stream cipher. *Proc. ICCASM 2010 - 2010 Inter. Conf. on Computer Application and System Modeling*, 7 (2010).
10. Kumar, P. and Pateriya, P.K., RC4 Enrichment algorithm approach for selective image encryption. *Inter. J. of Computer Science & Communic. Networks*, 2, **2**, 181-189 (2012).
11. Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. (2nd Edn), Network. 623-631 (1996).
12. Yu, Q. and Zhang, C.N., RC4 state and its applications. *Proc. 2011 9th Annual Inter. Conf. on Privacy, Security and Trust*, 264-269 (2011).
13. Koopahi, E. and Borujeni, S.E., Secure scan-based design using Blum Blum Shub algorithm. *Proc. 2016 IEEE East-West Design and Test Symp.* (2017).
14. Rahim, R., Winata, H., Zulkarnain, I. and Jaya, H., Prime number: an experiment Rabin-Miller and fast exponentiation. *J. of Physics: Conf. Series.*, 930, **1**, 12032 (2017).
15. Guo, M., Bhattacharya, P., Yang, M., Qian, K. and Yang, L., Learning mobile security with android security labware. *Proc. 44th ACM Technical Symp. on Computer Science Education*, 675 (2013).
16. Setiabudi, D.H. and Tjahyana, L.J., Mobile learning application based on hybrid mobile application technology running on Android smartphone and Blackberry. *Inter. Conf. on ICT for Smart Society*, 1-5 (2013).