Development of NgeXTEA: a web based learning tool for cryptography algorithm

Development of NgeXTEA: a web based learning tool for cryptography algorithm

Irfan Syamsuddin [1*] and Alimin Daude[1]

[1]Center for Applied ICT Research, Program Studi Teknik Komputer dan Jaringan, Jurusan Teknik Elektro, Politeknik Negeri Ujung Pandang, Jl. Perintis Kemerdekaan Km 10, Makassar 90245, Indonesia

[*]Corresponding author's e-mail: irfans@poliupg.ac.id

Abstract. One of the issues in teaching information security in particular cryptography is lack of tools to facilitate students' understanding of related topics. The study specifically discusses the development of a web based learning tool for teaching symmetric cryptography in Indonesian language. The module is called NgeXTEA which contains a guide to the process of encryption and decryption in stages using Extended Tiny Encryption Algorithm (XTEA). The development of NgeXTEA including its features is presented. Based on several evaluations with various combinations of characters, it is finally concluded that NgeXTEA module works well as expected.

1. Introduction

Organizations such as business, industries and government are all facing cyber related risks due to the growing reliance on using information and communication technologies [1]. Considering such issues, ACM and IEEE have introduced the Information Assurance and Security (IAS) Knowledge Area (KA) to the Body of Knowledge in recognition of its critical role for computer engineering and science education to prepare students dealing with any risks associated with increasing world's reliance on information technology [2]. The main objectives of the approach is to provide world standard guidance for educational institutions that offers information security related courses to structure the curriculum with up to date knowledge, skills, and abilities to protect information and information systems and to guarantee Confidentiality, Integrity, and Availability (CIA) at all levels who strongly rely on computer and the Internet for daily tasks [3].

Although the importance of security concepts and applications have been regarded as vital requirements in the computer engineering and science disciplines, in developing countries many computer engineering and science programs at higher education levels are still lacking of security expertise and lab resources to answer the requirements [4]. Therefore, higher education admits it as a gap that must be filled by continuous efforts to provide supporting tools and teaching materials for students to gain adequate knowledge and skills in the area of information security [5].

Information Security course offered to students majoring Computer & Network Engineering, School of Electrical Engineering at the State Polytechnic of Ujung Pandang, Indonesia in the sixth semester. Similar to other courses that combine theory and practice, this course also requires a number of tools for laboratory exercises in order to help students understanding the given topic.

It usually takes long time and hard efforts to teach cryptography topics such as Symmetric Cryptography and Asymmetric Cryptography for students to gain understanding on the given topics. Several problems associated in this case such as limited class hours, low mathematical background of the students, and lack of available tools to help student getting hands on practice [6]. Unfortunately, those tools commonly jump to the conclusion, showing final result of encryption and decryption without describing how the final results are obtained step by step. As a result, it is difficult for students to understand mathematical calculation behind the cryptography algorithm [6,7].

In order to deal with the issue, a new learning module for Symmetric Cryptography topic is introduced. The learning module is named NgeXTEA which stands for "Ngerti XTEA" means understanding XTEA in Indonesian language. As might be inferred from its name, NgeXTEA module is based on a cryptography algorithm called Extended Tiny Encryption Algorithm (XTEA) as a foundation to understand mathematical calculation of Symmetric Cryptography. NgeXTEA module comes with an easy to use Graphical User Interface (GUI) which makes it a self-explainer learning tool for students to learn cryptography at their own pace [8].

2. Methods

In this study, the author adopts research and development methodology by referring to XTEA logical concept introduced in [9,10]. It is then represented in the form of pseudo code for both encryption and decryption processes in order to ensure its logical flow before going to the next step of coding the algorithm. The following table shows how both encryption and decryption of XTEA are represented in pseudo code.

Table 1. Pseudocode of XTEA algorithm.

Algorithm 1: Pseudo Code XTEA Encryption	***Algorithm 2: Pseudo Code XTEA Decryption***
Sum = 0; delta = 0x9E3779B9	Sum = 0; delta = 0x9E3779B9
for i = 0 to N do	for i = 0 to N do
v0+ = ((v1 << 4) xor (v1 >> 5) + v1) xor (sum + key[sum & 3])	v1− = ((v0 << 4) xor (v1 >> 5) + v0) xor (sum + key[sum >> 11 & 3])
sum+ = delta	sum+ = delta
v1+ = ((v0 << 4) xor (v0 >> 5) + v0) (sum + key[sum >> 11 & 3])	v0− = ((v1 << 4) xor (v1 >> 5) + v1) (sum + Key[sum &3])
end for	end for

Once pseudo code is clearly verified, the next step goes to developing the software or coding in PHP [11]. Figure 1 shows PHP code for encryption process of XTEA, while the decryption process in PHP code can be seen in figure 2.

```
protected function xtea_encipher( $v0 , $v1 )
{
 $num_rounds = $this->_xtea_num_rounds;
 $sum = 0;
 echo "<table name='inimitabelnya' style='float:left;'>";
 echo "
<tr>
 <th scope='row'>V0</td>
  <th scope='row'>V1</td>
</tr>";
 do {


 // calculate ((($v1 << 4) ^ (($v1 >> 5) & 0x07FFFFFF)) + $v1)
 $v0a = $this->binadd((($v1 << 4) ^ (($v1 >> 5) & 0x07FFFFFF)) , $v1);
 // calculate ($sum + $this->_xtea_key[$sum & 3])
 $v0b = $this->binadd($sum , $this->_xtea_key[$sum & 3]);
 // Calculate ($v0 + ((($v1 << 4) ^ (($v1 >> 5) & 0x07FFFFFF)) + $v1)
 //            ^ ($sum + $this->_xtea_key[$sum & 3]))
 $v0 = $this->binadd($v0 , ($v0a  ^ $v0b));

 //Calculate ($sum + $this->_XTEA_DELTA)
 $sum = $this->binadd($sum , $this->_XTEA_DELTA);

 //Calculate ((($v0 << 4) ^ (($v0 >> 5) & 0x07FFFFFF)) + $v0)
 $v1a = $this->binadd((($v0 << 4) ^ (($v0 >> 5) & 0x07FFFFFF))  , $v0);
 // Calculate ($sum + $this->_xtea_key[($sum >>11) & 3])
 $v1b = $this->binadd($sum , $this->_xtea_key[($sum >>11) & 3]);
 //Calculate ($v1 + ((($v0 << 4) ^ (($v0 >> 5) & 0x07FFFFFF)) + $v0
 //           ^ ($sum & $this->_xtea_key[($sum >>11) & 3]))
 $v1 = $this->binadd($v1 , ($v1a  ^ $v1b));
 echo "
```

Figure 1. PHP code of XTEA encryption

```
protected function xtea_encipher( $v0 , $v1 )
{
 $num_rounds = $this->_xtea_num_rounds;
 $sum = 0;
 echo "<table name='inimitabelnya' style='float:left;'>";
 echo "
<tr>
 <th scope='row'>V0</td>
  <th scope='row'>V1</td>
</tr>";
 do {


 // calculate ((($v1 << 4) ^ (($v1 >> 5) & 0x07FFFFFF)) + $v1)
 $v0a = $this->binadd((($v1 << 4) ^ (($v1 >> 5) & 0x07FFFFFF)) , $v1);
 // calculate ($sum + $this->_xtea_key[$sum & 3])
 $v0b = $this->binadd($sum , $this->_xtea_key[$sum & 3]);
 // Calculate ($v0 + ((($v1 << 4) ^ (($v1 >> 5) & 0x07FFFFFF)) + $v1)
 //            ^ ($sum + $this->_xtea_key[$sum & 3]))
 $v0 = $this->binadd($v0 , ($v0a  ^ $v0b));

 //Calculate ($sum + $this->_XTEA_DELTA)
 $sum = $this->binadd($sum , $this->_XTEA_DELTA);

 //Calculate ((($v0 << 4) ^ (($v0 >> 5) & 0x07FFFFFF)) + $v0)
 $v1a = $this->binadd((($v0 << 4) ^ (($v0 >> 5) & 0x07FFFFFF))  , $v0);
 // Calculate ($sum + $this->_xtea_key[($sum >>11) & 3])
 $v1b = $this->binadd($sum , $this->_xtea_key[($sum >>11) & 3]);
 //Calculate ($v1 + ((($v0 << 4) ^ (($v0 >> 5) & 0x07FFFFFF)) + $v0
 //           ^ ($sum & $this->_xtea_key[($sum >>11) & 3]))
 $v1 = $this->binadd($v1 , ($v1a  ^ $v1b));
 echo "
```

Figure 2. PHP code of XTEA decryption

Every round of XTEA processes (both encryption and decryption) is clearly explained with clear comment line. In addition, each round result always treated as variable which value is then showed through the GUI of NgeXTEA in order to let students comparing the simulation results with their manual calculations at every round for both encryption and decryption. This is considered as the main feature of NgeXTEA which makes it understandable and user friendly even for those who never learn cryptography before.

Once both encryption and decryption processes of XTEA successfully tested with different combination of alphabet and numeric inputs, the next step is embedding it into the learning module and integrate it with all components to structure the NgeXTEA. The process of integration and user interface design are done using PHP, Javascript and CSS [11,12].

3. Result and Discussion

The main user interface (UI) of NgeXTEA is represented in figure 4. All instructions, text menu and text buttons are currently only available in Indonesian language [13]. NgeXTEA's simple UI design has an intuitive look and feel which clearly aid users get the idea of what the application is for.

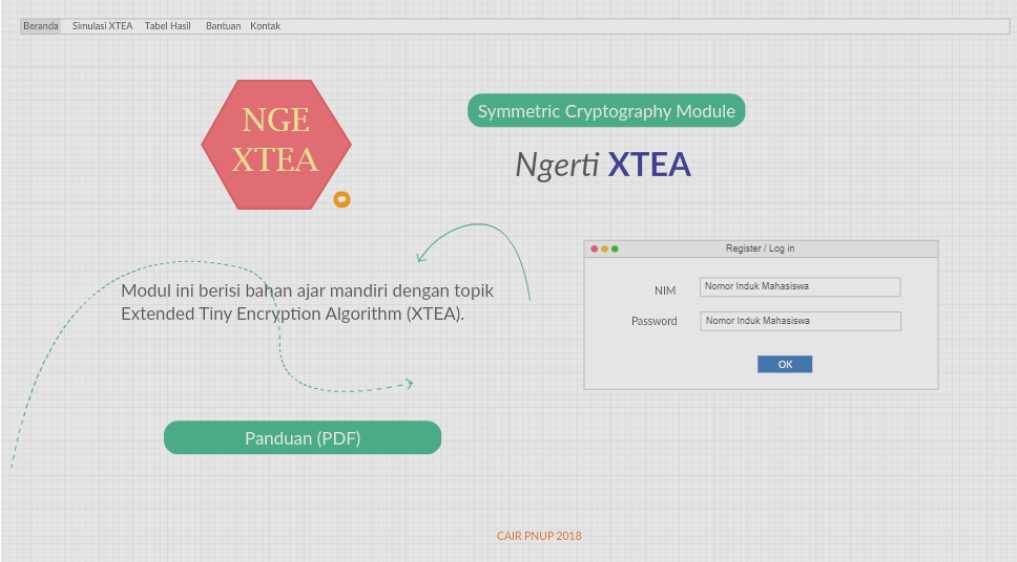

Figure 3. User interface of NgeXTEA

NgeXTEA provides several menus that will provide specific function according to which task needed by student as the user later. The menus are XTEA simulation, XTEA table of results, guidance and contact [13].

In the simulation menu, there are two options encryption mode and decryption mode. Student will be prompted to first mode of encryption by inserting "Plaintext" and "Key" into the given textboxes (in case of encryption). Then, it will direct the user to the next menu of "Tabel Hasil" showing the results of all rounds from "Plaintext" to "Ciphertext".

Besides, it also has a link of "Panduan (PDF)" which is a practical documentation in PDF format or the guideline on how to use the application as well as XTEA concept in Indonesian language. The guideline provides students with everything they need to understand how XTEA algorithm.

Another important point is by following the guideline (i.e. Panduan PDF), student will be guided in steps for conducting manual encryption process whether by MS Excel or MS Calculator. Conversely, students will be able to do manual decryption process using MS Excel or MS Calculator to convert the "Ciphertext" into the "Plaintext" in step by step processes. Their manual calculations could be compared with NgeXTEA results.

In order to improve student understanding, the guideline suggests supplying three different plaintexts (text only, number only and combination of text and number) with different keys to find out how XTEA deals with various plain text. Then, students should perform manual calculation and compare their

results with automatic calculation by NgeXTEA module. Table 4 shows the evaluation results of encryption and decryption of NgeXTEA module.

All results obtained by students are combined to create report provided by NgeXTEA guideline. The report then submitted to the lecturer via email textbox provided in "Kontak" menu.

It is found that the module performs positive results on various inputs and key length where both encryption and decryption successfully done. It is found that using the same key, user may encrypt any given plaintext and vice versa.

Table 2. Evaluation results of NgeXTEA.

Encryption	***Decryption***	***Key***	***Result***
Politeknik	wRx8cDN+vWfaI6UtW+sq96PUVqbclib/	123	Ok
politeknik	C3DoyNuQyOy0haINqaS4Hb6rqXTJZkLBiM37NQw	123	Ok
negeri ujung pandang	GiiGe+rCxFs9S6Q==		
makassar kota daeng	2zyM8/33j59t3OPRD4gIuPqaJ2p4dpHdk/r5wVdVDu4=	82716514414	Ok
sulawesi	E8fKhrv8evDGXS3p1IJEtwBhMolpsTD910BlOJak+Ss=	82716514414	Ok
pa'rasanganta'			
120021998	24JP6eHHOOr+AG5yfgOMncXJkV6gll1i	1920	Ok
28736155172992	AaCx8QwSa6xbeVT5m9ag2pyPGiVIlxJB	1920	Ok
362525272541	YN266FlDB7fKjhdYZf/DSmuHVXTWnehs	7465243	Ok
perintis km 10	HEuHjPCGblnywZsTCKwCl/5nG/sfBBWG	29834736	Ok
tamalanrea	M+pBpofI/C6yu8383y3RcJ2xFPCI42jf4v28/U0MA3l	92081726518	Ok
blok M3 No 452634	Hm2PnviIS/Q==		
17 agustus 1945	5Lgp8Zukuk5Q2NJVMuXKc6wS3ohBFJvg	92081726518	Ok
b1sm1ll4h	WDFBlqHjXIw0fh1ZzeDvM3NNLQDrmKOB	46353	Ok
t3kn1k	j9Phh2Yas/IcYH2UVxxx7JnA4aqWXZz471f9SsFQh	837621612514	Ok
k0mput3r	ws=		
j4r1ng4n			
c3nt3r f0r	14qCl4WiNEF+1tzwL2PK346ou4eIh9xG2iMDUjwU	6437363528	Ok
4ppl13d 1ct	UzVjGHCDnKjx+w==		
r3s34rch			
P@$w0rd	rOh2+6KU0o+jh0+EE8MsgA==	87803	Ok
s3&o0r!	3rHjV1K8K2oywpLFaM6+ww==	9234	Ok

The technical evaluation of NgeXTEA indicates the applicability of NgeXTEA to use as teaching module for symmetric cryptography topic which is also in accordance with previous study [13].

In the future, this study will be extended in two ways. Firstly, considering its small size and strength in algorithm, XTEA might be applied for mobile cloud computing security such as secure chat for mobile government [14].

Secondly, NgeXTEA will be improved by making it available in different language options such as English, Arabic and Chinese before releasing it to public as open source software [15] for wider adoption in the world.

4. Conclusion

A new learning module called NgeXTEA is developed and introduced in this study. It is intended to fill up the gap of easy to use cryptography tool to assist student in understanding how Symmetric Cryptography works in particular Extended Tiny Encryption Algorithm (XTEA).

NgeXTEA learning module is developed with PHP and Javascript which can run in any modern browsers. Student may refer to the guideline (i.e. Panduan PDF) in the module to follow the steps for conducting XTEA simulation as well as manual cryptanalysis with MS Excel or MS Calculator. Final report of each student might be obtained by the lecturer through submission link provided in the module. Thorough testing of NgeXTEA reveals that it adequately performs both encryption and decryption processes in various types of input such as alphabet, numeric or combination of both in different key length.

For further research, we aim to implement XTEA for mobile communications security and another plan is to enrich the module by translating it into different languages for more adoptions.

5. References

[1] Oulasvirta L and Anttiroiko A 2017 Adoption of comprehensive risk management in local government. Local Government Studies **43** pp.451-474.
[2] ACM/IEEE-CS 2013 Computer Science Curricula 2013, https://www.acm.org/education/CS2013-final-report.pdf accessed on 11 April 2019.
[3] Olejar, D & Stanek, M. 1999 *In IFIP WG* **11** pp. 1–9.
[4] Elnajjar A E A and Abu Naser S S 2017 *International Journal of Advanced Research and Development* **2** pp 69-73
[5] Yuan,X, Vega P, Qadah Y, Archer R, Yu,H and Xu J 2010 *ACM Transactions on Computing Education* **9** pp.147–155.
[6] Adamovic, S, Sarac M, Stamenkovic D and Radovanovic D 2018 *International Journal of Engineering Education* **34** pp.256–262.
[7] Briliyant, O C and Baihaqi,A 2017 *11th International Conference on Telecommunication Systems Services and Applications (TSSA)* pp.12-21.
[8] Song, X and Deng,H 2009 *Proceedings of the First International Workshop on Education Technology and Computer Science* **2** pp. 490–494.
[9] Wheeler D J and Needham R M 1994 *International Workshop on Fast Software Encryption* pp. 363-366.
[10] Needham R M and Wheeler D J 1997 Tea Extensions. Report, Cambridge University.
[11] Baatard, G 2007 Australian Information Security Management Conference p. 21.
[12] DiPierro M 2018 Computing in Science & Engineering **20** pp 9-10
[13] Syamsuddin, I. 2018 *Global Journal of Engineering Education* **20** pp 196-200
[14] Syamsuddin I and Hwang J 2010 *IEEE International Conference on Application of Information and Communication Technologies* pp 1-5
[15] Tang Y and Zhou Q 2009 *4th International Conference on Computer Science & Education* pp 1604-1608