Cryptography Related to Children Education

Ranindya Paramitha 13516006[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13516006@std.stei.itb.ac.id

***Abstract*— Cryptography is a science and art that using modular arithmetic to secure messages by encrypting it into another unreadable text and decrypting it back. Cryptography has been used in many technologies. Cryptography also developed into a puzzle called cryptogram. Cryptogram is a genre of puzzle that applying cryptography and there are some that could be solved by children. Cryptography as cryptogram has many benefits for children, such as enhancing critical thinking skill, hand-eye coordination, concentration rate, problem solving skill, etc. Cryptography is also used in IQ-Test to test cognitive abilities.**

***Keywords*—Children, Cryptogram, Cryptography, Education.**

I. Introduction

Number theory is a part in discrete mathematic which learns about integers. Number theories, especially modular arithmetic and prime numbers, are basic for many things in computer science world, including cryptography. Basically, cryptography is a science that is encrypting some message to a cipher-text and decrypting it back to read it. Basic cryptography uses modular principle in their formula to generate a cipher-text from a readable one and decrypt it back so the information transfer would have increased security. Nowadays, people also could encrypt pictures and not only texts.

Cryptography is used anywhere in this world, especially for many security problems. Password security, IP security could make use of cryptography. Some information sharing in World War II even using cryptography to keep their information secure from their enemies. Therefore, cryptography is not used for solving security problem only. Cryptography has influenced many areas of knowledge, including children education. Here are some examples of how people use cryptography in education: Cryptography is used as a part of Standford-Binet Scale Fourth-Edition IQ-Test in the section of verbal reasoning. Cryptography also develops to a puzzle genre, called cryptogram. It basically is a puzzle game using cryptography in the form of words or pictures.

Children are future leaders. They are being built by education. Children education is an important thing. Education that brought by parents, teachers, could shape the future of children, because they teach knowledge, attitude, etc. that would help children later when they have to work and survive. What children learnt in their young ages, could determine their future. Therefore, sometimes education with bad delivery and application would make the students feel bored, especially in formal education. Sometimes, students need activity that could bring their interest to their study topics. This paper would discuss more about how and why teacher could use cryptography (or cryptogram) in education.

II. Theories

2.1 Number Theory

Number theory is a part of discrete mathematic which studies about integers [14]. Integers are numbers which has zero decimal point. This section would discuss more about division property of integer. Division property of integer says that if n and m are integers with $n \neq 0$, then when m is divided by a there would be two unique integers q (quotient) and r (remainder, $0 \leq r \leq n$), therefore:

$$m = nq + r \quad (1)$$

Division property of integer later generate modular arithmetic and prime numbers theories.

2.1.1 Modular Arithmetic

Modular arithmetic plays a big role in integer calculation, especially in cryptography which would be discussed in the next chapter. Modular arithmetic uses *mod* as its operator. Mod is an operator that gives the remainder of integer division. Therefore, $a \bmod m = r$ means $a = mq + r$, with $0 \leq r < m$. If there are two integers a and b, they could be said *congruent* in modular m, if only they have a same remainder when they are divided by another integer m. Congruence could be written as:

$$a \equiv b \pmod{m} \quad (2)$$

In other words, *a congruent b* in *modular m* means m could divide $a - b$. Equation (2) could b written as another equation:

$$a = b + km \quad (3)$$

Theorems for modular arithmetic where m is positive integer:

a. If (2) true and c is integer then:
   i. $(a + c) \equiv (b + c) \pmod{m}$ (4)
   ii. $ac \equiv bc \pmod{m}$ (5)
   iii. $a^p \equiv b^p \pmod{m}$ for a non-negative integer p (6)

b. If (2) true and c *congruent* with d in *modular m* then:
   i. $(a + c) \equiv (b + d) \pmod{m}$ (7)
   ii. $ac \equiv bd \pmod{m}$ (8)

Two integers a and b are called prime relatives if their greatest common divisor is 1. If a and m are prime relatives and $m > 1$, then invers from $a \bmod m$ could be defined. Modulo invers could be written as:

$$a\bar{a} \equiv 1 \pmod{m} \quad (9)$$

There is also linear congruence. Linear congruence is written as:

$$ax \equiv b \pmod{m} \quad (10)$$

with m is a positive integer, a and b are integers and x is integer variable. Linear congruence is defining values of x which fit the congruence equation.

2.1.2 Prime Numbers

Prime numbers are positive integers greater than 1 that only divisible by 1 and itself. Other number that is not prime number is called composite. The fundamental theorem of arithmetic says that: every positive integer that is greater than or equal with 2 could be declared as result of multiplication from 1 or more primes. To test is a number prime or not we could use Fermat Theorem (especially for big numbers): if p is prime and a is integer that could not divided by p (greatest common divisor of p and a is 1) then:

$$a^{p-1} \equiv 1 (\text{mod } p) \quad (11)$$

2.2 Cryptography

Cryptography is a science and also an art of securing a message so it content would be kept as a secret by encrypting it into a code form that does not has any meanings. Nowadays, security of a message is very important, therefore, cryptography is used to secure messages so people who do not have the right to access it could not read the message. Only person or people who have the right to access the message could read the message because they have the key/ methods to decrypt the message to the readable form.

A plain text is message that want to be secured. A cipher-text is a text without meaning as a result of encrypting the plain text. Encryption is a process to disguise a plain text to a form that does not have a meaning. While decryption is a process to translate a cipher-text back to a readable plain text. Nowadays, cryptography is used in computer security system, such as data keeping in the disk storage and data sending from one place to another. Data that stored in a disk storage is stored as cipher-text, and only the rightful person who could decrypt it back. In data sending processes, data is being encrypted before transmitted to the receiver, and only in the receiver device the data could be decrypted back to its original form.

2.2.1 History of Cryptography

The word cryptography itself came from Greek words: *kryptos* which means 'hidden' and *graphein* which means 'writing'. Since 1900 BC, Egyptian scribes has used hieroglyphs that is assumed hiding some meaning from people who did not know the meaning. Later, around early 400 BC, Greek Sparta soldier wrapped tape around a stick, then wrote message on the wound stick. After that, they unwound the stick, so the message on the tape would be unreadable and meaningless. This equipment is called *scytale*.

Fig. 01 Scytale Cypher
(Source: http://www.oxfordmathcenter.com/drupal7/node/486)

Person who wanted to figure out the meaning had to have a stick/ cylinder with the same diameter with the sender's then he/ she had to wrap the message tape to the stick so he/ she could read it. This cryptography technique is called cipher transposition. Not only Egyptian and Greek, Roman also had their own technique, called Caesar Shift Cipher. The idea was shifting letters by numbers that they had agreed about and then write the message using that shifted letters. The receiver needed to shift letters back to make the message readable. This cipher is an example of Monoalphabetic Cipher.

If there were monoalphabetic teechniques, there must be the polyalphabetic one. It was developed by Leon Battista Alberti, whom then known as "The Father of Western Cryptology". He was using two copper disks that fit together. The disks had alphabets inscribed on it. After a few words, he rotated the disks so the encryption logic would be changed. This type of cryptography was mentioned to be used in Civil War.

2.2.2 Cryptology

Cryptology is a study about cryptography and cryptanalyst. Cryptanalyst itself is someone who learn about encryption methods and cipher-texts with a goal, which is to find the plain text form of the cipher-text. Someone who make the cipher-text (encrypting a plain text to a cipher-text that would be decrypted by a cryptanalyst) is called a cryptographer.

2.2.3 Notation and Algorithms

Encryption could be notated by:

$$E(P) = C$$

With E is encryption, P is plain text, and C is cipher-text. Instead, decryption could be notated by:

$$D(C) = P$$

With D is decryption, P is plain text, and C is cipher-text. Cryptography algorithm (cipher) is a mathematic function for decrypting and encrypting a message. The strength of an algorithm is calculated from how much work needed to translate a cipher-text into its readable plain text form. Time to break the code could also determine the strength of an algorithm. More time needed to solve a cipher-text to it plain text form, more work needed to solve the algorithm, means the algorithm has a good strength and has better security.

Restricted algorithm is an algorithm that strength determined by keeping it as a secret. Modern cryptography is not using restricted algorithms. It algorithm could be known by public. It strength is located on its key, which is a code, usually a row of integer, that is kept as a secret. The message could only be encrypted or decrypted by people who know the key. This key has similar function with password in computer system and pin in bank cards.

When encrypting key is equal with the decrypting key, the cryptography algorithm would be called symmetric algorithm. Data Encryption Standard (DES) is an example of symmetric algorithm. This algorithm also called as private key algorithm, because the algorithm is needed to be kept as a secret. This algorithm's weakness is that the sender and receiver must have the key, which means the sender needs to find a way to tell the key to the receiver. Otherwise, when the encrypting key is not equal with the decrypting key, the cryptography algorithm is called non-symmetric algorithm.

Rivest-Shamir-Adleman algorithm is one of its example. This algorithm is also called by public key algorithm. It has two keys, one public key (known by public) for encryption and one secret key (known only by receiver) for decryption.

2.3 Cryptogram

According to Merriam-Webster Dictionary in [13], cryptogram could be explained as a way to communicate with other people using code. According to Danesi in [4], cryptogram became very popular in the nineteenth century. A writer, Edgar Alan Poe, used cryptogram to make the plot of his story, The Gold Bug (1843). After this story, cryptogram has also used as basis of many mystery stories, such as Jules Verne's La Jangada (1881) and Maurice Leblanc's The Hollow Needle (1910). Even Sir Arthur Conan Doyle also sometimes used cryptograms in his stories.

Cryptograms has developed to some forms, but the most common one is similar to Caesar Cipher Cryptography, which is using letter-to-letter substitution.

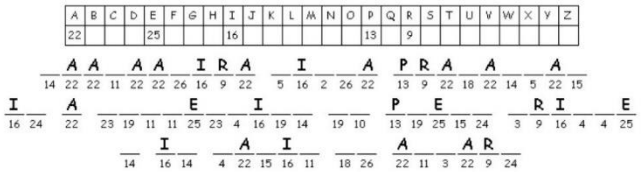

Fig. 02 Example of Cryptogram Puzzle
(Source: http://anudinam.org/2013/10/28/89096/)

2.4 Children

According to Oxford Living Dictionaries in [7], a child is a young human being below the age of puberty or below the legal age of majority. Children is a plural form of child.

2.5 Education

Education, according to Merriam-Webster Dictionary in [13], is defined the action or process of educating or of being educated. Education has many forms, but people usually generalize education into three major forms: formal education, informal education, and non-formal education [5].

2.5.1 Formal Education

Formal education is usually held in a classroom, taught by a educated teachers. Teachers have to fulfill a standard of their educational skill and stick to a specified given curriculum. Formal education is well-planned, it is also limited to a specific amount of time. Formal education is strict about discipline.

2.5.2 Informal Education

Informal education usually happens outside the classroom, it may be at home, after-school activities, organizations, libraries, etc. It is usually not-pre-planned. Informal education is rarely has prescribed time-table or curriculum. It could be spontaneous, and usually not imparted by any specialized agency.

2.5.3 Non-Formal Education

Non-formal education is an education that arranged and organized consciously and systematically. Therefore, unlike formal education, which is usually organized by the government and/or using a standard curriculum from the government, non-formal education is organized for a homogenous group to learn something in particular. In other word, non-formal education is serving the need of a particular group, for example: for those who want to learn English, there are English courses, for those who want to learn how to cook, there are cooking courses, etc.

III. Relation of Cryptography and Children Education

3.1 Relation of Play and Recreation with Education

Playing in education is usually related with education in kindergarten [9]. In kindergarten, playing is used as a method for developing mental and spiritual. Therefore, if we could find a reason (biologically, psychologically, etc.) to use playing as a method of education in kindergarten, then the same reason holds for all periods of children growth and development in education. It is inconsistent if we accept a method for one period of education but ignore it for other periods of children growth.

Sometimes, there is an excuse that in kindergarten, children play because it is the subject matter in kindergarten, which other school periods above it do not accept. Subject matter in schools are basically inherited from older generations. It was what generations in the past interested in, or activities and achievements that that generation had. Children in today's education, inherit this subject matter, so they are pushed to learn the subject matter and then build their interests, activities, and achievements. Therefore, according to George E. Johnson in his book titled *"Education through Recreation"*, an efficient method for education is building the subject matter from children's interests, activities, and achievements, and not the reverse.

Human brain cells are created practically all complete, but the connections among the cells have yet to be established. Brain is like other organs. According to George Herbert Mead, in his paper titled *"The Relation of Play to Education"*, when an organ is fully and normally developed, an exercise that is involved entire interests and processes is needed for it, and play is the application of this principle to the development. In play, organs that yet to be fully developed, are given exercises, but it never directing to the end purposes which the organ may not be able to do with it capacity in the current condition.

In Reference [12], Mead said that what children could do is naturally his/her interests and does not need a continuous boosting. Some right stimulus are needed to grab that spontaneous use of coordination, and play is that stimulus. For example, using coins for simulating economy transactions in buying and selling game. It maybe not showing the real buying and selling nature, but it could call the nature of it from inside children.

The problem is finding the right and appropriate stimulus to naturally called children activities and interests, and not forcing children to work where he/ she has no interest. Then, the solution is giving a child the right environment to study, where he/ she finds what make him/ her interested. Nowadays, educations may be not giving the right stimulus for all children, forcing its own interests to some children which maybe have interests in other field. This could have a fatal effects, such as losing concentration. Our job is not forcing children to our own interests or past generations' interests, but organizing and arranging the right stimulus for every child in order to fulfill their natural interests.

Therefore, no one could change the education system that has worked nowadays entirely. Nowadays, children are required to

join formal educations with specified curriculum which maybe not the best fit for every child interests. Moreover, when children are forced to study fields that they are not interested in, they would be bored, losing their concentration, and somehow, this would make them scolded by teacher who does not aware that the kid actually has natural interests in other field. The scolding could make children afraid, and they would try to force themselves to do things that they are naturally not interested in, which could cause confidence losing and even stress. Playing and doing activities instead of reading text books and listening to what teachers are saying (just like teachers are always right) actually would help adults to know what things that made children interested with, and also bring back the concentration and respect from the children because they would be more interested on what they should learn.

3.2 Puzzle Benefits for Children

Puzzle is basically a game or problem designed to test knowledge. Puzzle usually needs effort and patient to be solved. Puzzle could be used for games (amusement) or even a knowledge test. Puzzle has some benefits for children:

3.2.1 Enhancing Hand-Eye Coordination [15]

When children play with puzzle, they need to look at puzzle pieces, take it, and place it in the right place that they have seen before. In other type of puzzle, word game, children need to look at words and they need to either arrange the words into the right order or write the answer in the correct place. This kind of activities would enhance children's hand-eye coordination, because they demand quick reaction from hand to do something when eyes are looking at some puzzle pieces/ words that looks fit with a place.

3.2.2 Enhancing Memory [15]

When children play with puzzle, they need to remember the shape, the size of puzzle pieces. When a puzzle piece is not fit with a place, they need to set it aside but also remember its property so when they finally find the right place, they has had the memory of the puzzle piece. The same with word game. Children would try to remember what word or letter that suit the place, instead of checking in every step they made to solve the puzzle.

3.2.3 Developing Problem Solving Skills [15]

When a children play with a puzzle, they are actually facing a problem. They need to solve the puzzle, placing all pieces on the right place. They have to think how to solve the puzzle, the strategy to find the best fit piece for a place, finding right connection among pieces. Absolutely, this is far from problems that human faced every day, but at least, when children play a puzzle, they learn that there are problems that need to be solved, and they learn that they have to be involved solving problems that occur in everyday life. In the word game, children are facing a problem that they could not understand a message so they need to solve it by placing words or finding words that match with a sentence. This game trains children brain to react wisely when facing a problem. Puzzles sometimes also teach children that in some problems, we need trial and error, but we should keep trying to solve the problem.

3.2.4 Teaching Children Setting Small Goals [15]

Playing puzzle has a goal, either it is finishing the puzzle, with all puzzle pieces in the right place, making a sentence, making a picture, or other small goals. When children play a puzzle, they need to be clear about the goal. Usually, adults tell them that they have to arrange the order of puzzle pieces/ words to see the full picture/ sentence. Here, in the children brain, they are setting a goal, that they want to see what picture/ sentence would be made. Begin with a desire, they work and try to solve the puzzle. This is actually a simple way to teach children that in life, we need a set a goals that we want to achieve. Therefore, to achieve that goals, we could not just lean back, but we need to work and make some efforts for it.

3.2.5 Making Learning Activity Fun

Puzzle could make learning activity more fun. For example, for children who learn about human body, they could play puzzle that arranging human organs in the right place while memorizing it names and function. Another example is learning vocabularies using puzzle, with words and picture pieces then children could arrange the right word with the right picture and also learning geography by using world map puzzle, so the children have to arrange the world map while learning about the country's name, president, etc. With this kind of activity, children would be easier to understand where is exactly an organ is located in human body, what the name of an object is, and what information they should learn about a country and where it is exactly located in the earth. Puzzle could also be challenging. It challenges children to think and solve the problem. Being challenged is somehow fun and exciting for children. They could be more passionate to learn when they are faced with activities like solving puzzles than when they need to read many text books all day long.

3.2.6 Increasing Concentration Rate

When playing puzzle, children need to put their concentration to the puzzle. Their brain are forced to concentrate, memorizing pieces/ words that they should arrange and finding the right place. This activity would train children to be fully concentrate with what they do to achieve their goals. When they are distracted to other things, they would be realized that when they back to the puzzle, they need more efforts to recall what they have remembered before. This situation would make children think that it is better to concentrate for a little time than wasting time that would need more efforts to solve the same problem.

3.2.7 Repelling Boredom of Studying

Nowadays, education has had a specified curriculum that include some fields that may not suit every child. Lacking of interest in one subject could make children feel bored with the subject, and worse, they may not want to study the subject. Using games, especially puzzles that have many benefits for children, could be an alternatives. When children are bored to read text books, memorizing things from the book, playing games and puzzles would repel the boredom. Children would be brought back to their nature to play, so they should be more interested to puzzles. Using different methods of learning and teaching could help children to be interested with subjects and topics that they need to learn about. When children are interested to the subject, it would be much easier for them to understand and memorize the subject.

3.2.8 Teaching Moral Values

One moral value that is taught when children play puzzle is to fight and not giving up easily. Playing puzzle

demands children to try and try again, until they find the right piece for the right place. They usually need to try more than one time, and here, puzzles also teach children that sometimes they maybe fail, but there are chances to try, so they need to get up and try again. Children are also taught to be precise and not to be careless, because a puzzle piece/ a word is usually could fit only in one place. Children could learn that in everyday life, they should arrange their stuffs nicely, and put their activities and stuffs in order to make their life easier so they could achieve their goals.

3.2.9 Pattern Recognition Skill (Visual)

Playing puzzle demands children to look at patterns of puzzle pieces, sentences and words, etc. This would increase children's visual observing skill, when they try to put the right piece on the right place. They need to look at pattern to make their work easier. This skill would be useful when in their life children would meet many people with their own pattern and personalities. Children are taught that there are many patterns in the world that they should know and observe.

3.3 Cryptogram Applications as Puzzle

Cryptogram is one genre of puzzles that applies cryptography, where children have to solve a cipher-text/ picture using a set of key that is given for solving the cipher-text. Usually, children need to match letters in the cipher-text with letters in the key set. After that, children need to write/ place the plain text letter that they have got by matching the key in a place so when they are finished matching all letters, they could read the message. Actually, the children are given a task to decrypt a cipher-text to its readable plain text.

Cryptogram is also called cryptoquote. Cryptogram has some advantages. The first one is it is fun. Children are usually curious what is the meaning or the message that hidden in a cipher-text. It is challenging and fun for children, and they are usually satisfied when they could find the message. Moreover when this cryptogram solving is included in a set of game. Besides, solving cryptograms could increase children's critical thinking skill. Critical thinking skills is made up from many skills that help children to make a decision. When solving cryptograms, children need to analyze the cipher-text and the key, and sometimes using the result to solve bigger problem.

Here are some cryptogram applications for children:

3.3.1 Fact or Fiction

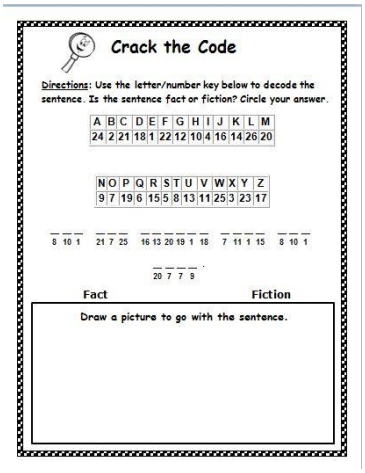

Fig. 03 Fact or Fiction Cryptogram
(Source: http://readyteacher.com/cryptogram-fact-or-fiction/)

In this cryptogram, children have to match numbers below underline to the key box in the above, and fill the blanks with a letter matched with the number. In this cryptogram, the answer should be "*The cow jumped over the moon"*. After finding the right sentence, children are instructed to decide is it a fact or fiction and then draw an image that describe the sentence. This activity would test children's comprehensive reading skills, numbers and letters recognition, knowledge about fact and fiction, critical thinking (deciding whether it is fact or fiction), and also let them having fun when solving the cryptogram and drawing a picture related to their decrypting result.

3.3.2 Cryptogram about Penguins

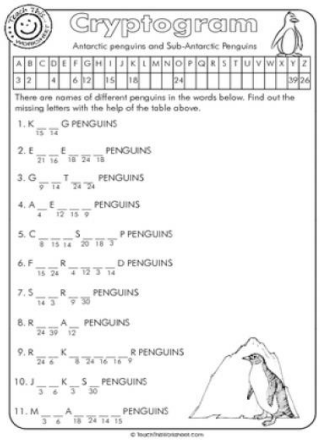

Fig. 04 Cryptogram about Penguins
(Source: http://www.teachthisworksheet.com/static-worksheets/antarctic-cryptogram)

A cryptogram could also be an alternative for teacher when teaching subjects that require children to learn new vocabularies. The picture above is one example. In the picture above, children have to fill in the blanks with the suitable letter according to key box. When they have filled all the blanks, they would find eleven penguin names. This way is more fun because children could find information by themselves and not just waiting to be told by the teacher. This method could be effective especially for children who do not like to memorize many vocabularies. Writing, matching letter, and solving the cryptogram would push children brain to work so it could memorize things easier.

Still about penguins, cryptogram could also be used to introduce penguin facts to children:

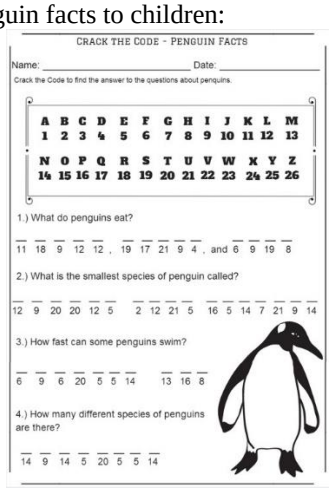

Fig. 05 Cryptogram about Penguin Facts

(Source: http://www.miniaturemasterminds.com/2015/01/14/crack-the-code-penguin-facts-codebreaker-worksheet/)

This cryptogram helps children learn about natural science especially about penguins, in the fun way. After this activity, children would be satisfied that they could find facts about penguin themselves by solving the cryptogram. This cryptogram would help children to be interested with natural science and facts about animals.

3.3.3 Cryptogram about Solar System

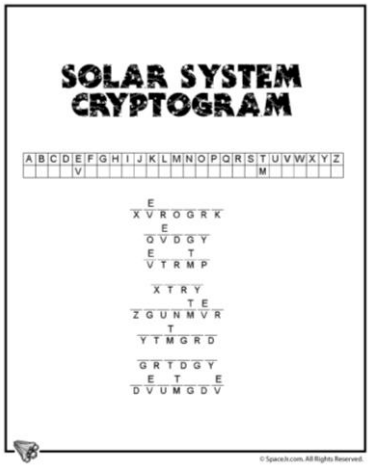

Fig. 05 Cryptogram about Solar System
(Source: https://www.woojr.com/solar-system-for-kids/planets-cryptogram-2/)

Unlike other cryptogram that using numbers, this cryptogram is using Caesar Cipher Cryptography, which shift letter with a secret number to make the cipher-text. Here, children have to fill the key box after analyzing the clues given. After filling the key box, they only have to match the letter under the blanks with the letter in the key box and write the corresponding letter in the blanks. In this cryptogram, children would learn about planets in the solar system. Therefore, while solving cryptograms, children would either be told or reminded about what they have learnt before about planets name. This method could help children memorize planet names.

3.3.4 Cryptogram about Mood Vocabularies

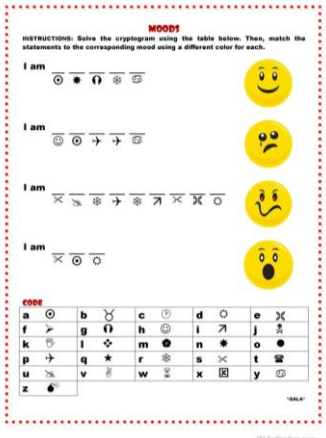

Fig. 06 Cryptogram about Mood Vocabularies
(Source: https://en.islcollective.com/resources/printables/worksheets_doc_docx/moodsfeelings_for_little_children/adjectives-feelings-feelings/22483)

While other cryptograms are using words, letters, and numbers, this cryptogram is using symbols to encrypt the plain text. Symbol cryptograms like the picture above, train children to look at patterns. It is increasing children's visual observing skill. Above cryptogram teaches about vocabularies about types of mood. Children are asked to write a suitable letter that correspond with the symbol below the underline by matching it with symbols and letters in the key box. After the decryption process, children would know what expression does the emoticons express called.

3.3.5 Cryptogram for Finding Information

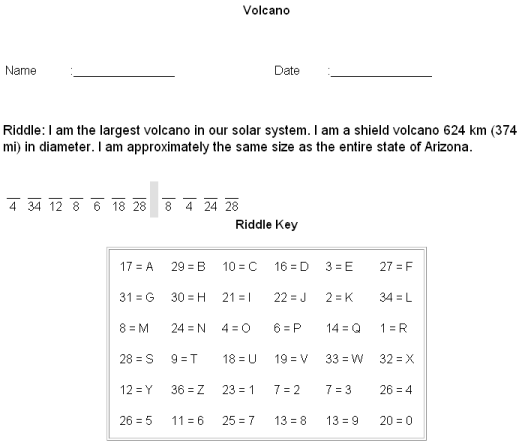

Fig. 07 Cryptogram for Finding a Volcano Name
(Source: http://www.makeworksheets.com/samples/puzzles/secretdecode.html)

The picture above is an example of using cryptogram for giving information to children. Therefore, children must make some efforts before they finally get the information. Here, children are taught that they need to fight and do something to earn something valuables. In the example above, children are given information about the largest volcano in the solar system. The cryptogram uses random number as the key of each letter, so this requires more concentration to solve it quickly.

3.3.6 Scytale Cipher

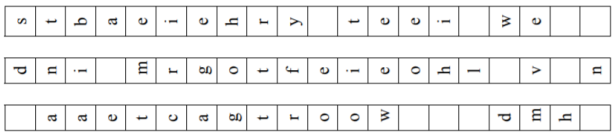

Fig. 08 Example of Syctale Strip
(Source: https://blossoms.mit.edu/sites/default/files/video/download/aurangzeb-activities.pdf)

Scytale cipher is an interesting activities for children. Children rarely see an object like scytale in the world nowadays. Therefore, when they are given strips of paper with meaningless arranged letters on it, their curiosity would be increased. They would want to know how to read the message. The message itself could contain many things, including new vocabularies and other educational stuffs. Teachers could ask their students to try finding object that they could wrap with the strip with the right diameter so they could read the message. This would make the learning activity fun and repel children boredom.

3.3.7 Vignere Cipher

Vignere Cipher is using a key word. Every letter in the keyword determines how many letters should be shifted from a plain text to make a cipher-text. For example, with a key word: "key". K is 11th letter, E is 5th letter, and Y is 25th letter [11]. Therefore, to encrypt a plain text to a cipher text, the first letter form the plain text must be shifted by 11, the second letter by 5, the third letter by 25, the fourth letter by 11, the fifth letter by 5, and so on. Children could be asked to encrypt a plain text to cipher-text or decrypt a cipher-text to a plain text. Here, children are taught to be careful while shifting letters using a keyword as a reference.

3.4 Cryptography Used in IQ-Test

Because of it benefits, that tested children concentration, visual skills, critical thinking skill, and other skills, cryptography is also used as one part of an IQ-Test called Standford-Binet Intelligence Scale 4th Edition. It is a standardized test for kids and adults from 2 years old to find out cognitive abilities and intelligence level of someone. The fourth edition of this test includes 4 score areas: Verbal Reasoning, Abstract/Visual Reasoning, Quantitative Reasoning, and Short-Term Memory [6]. Cryptography is one example for the test in Verbal Reasoning score area. This IQ-Test is considered as a very reliable test. The using of cryptography as a part of IQ-Test showed that cryptography is related with intelligence level. It could test word knowledge, awareness, and critical thinking of someone.

3.5 Introducing Cryptography in Security to Children

Cryptography is fun for children. Children usually know cryptography from cryptograms. Therefore, in the real world, cryptography is mostly used in security problems. Children should know that people nowadays have to secure their information because no one knows, maybe someone out there want to know about the information too, even when the information is actually private only for a group of people. Then, how to secure the information? Here, adults have the role to teach children about the use of cryptography to secure a secret information. There are many different approaches could be tried, therefore, this paper would only discuss two simple approaches.

In [11], there is an interested approach. This first approach is just for introducing about cryptography for security purpose to children. This approach is using a game to earn information about average weight of children in one class, without having every child announces their weight to all his/ her friends. The method starts by choosing a child, then this first kid chooses a secret integer, and add his/ her weight to the number. He/ she should pass the result secretly to a child beside him/ her that would add his/ her own weight to the number, and tell the result to a child beside him/ her, and so on until all children have added their weight to the number. Then the last children tells the final number to the first child that has to reduce the result with his secret number in the beginning and announce the result. This result is the sum of all children's weight, then the teacher could find the average by dividing with number of children in the class. After this activity, teacher could explain that they have demonstrated a simple message security using a simple secret key.

There is another approach in [1]. This second approach is explaining about how a message is securely transmitted from sender to receiver without sending the key. Here, the message is illustrated to be being secured in a box with 2 padlocks. The sender puts the message inside the box and secure it with one padlock. Then, the sender sends the box to the receiver. The receiver puts another padlock on the box and sends it back to the sender. When the sender accepts the box, the sender open his/ her own padlock and sends it back to the receiver. Finally, the receiver could open the box using his own key. This illustration is actually illustrates an asymmetric cryptography, but in the most simple way. With this illustration, children would learn that sometimes the sender could not pass the "key" directly to the receiver, so to keep the message secured, the sender and the receiver should think the way to have two different keys, one for encrypt the message and one for decrypt it. By having two different keys, they do not need to exchange key every time they want to send/ receive a message.

IV. Conclusion

To sum up, cryptography has many benefits for children education, especially for making learning activities more fun and enjoyable, and increasing many children skills. It is also beneficial to test children's cognitive abilities and introduce a common data security to children.

V. Acknowledgment

First and foremost, praises and thanks to God, for His blessings and kindness, so I could finish this paper.

I would like to express my deep gratitude to my lecturer Dr. Judhi Santoso, M.Sc. that has been taught me about discrete mathematics, especially number theories, modular arithmetic, and cryptographies. Without that basic knowledge, I must be confused when facing this task.

I also want to say thank you to Mr. Judhi and his colleagues in discrete mathematic lecturer team: Dr. Ir. Rinaldi Munir, MT. and Dra. Harlili M.Sc. for arranging this task so I could expand my knowledge and find one more computer science relation with my personal passions, children and their educations.

I thank all my colleagues, students of batch 2016 Informatics Major in Bandung Institute of Technology, for all the support.

Finally, I want to acknowledge with gratitude, the support and endless love from my family: my parents and my little brother. Without their smile and support, I think I could not make this up.

References

[1] Bultel, Xavier. Jannik Dreier. Pascal Lafourcade. Malika More. *How to Explain Modern Security Concepts to your Children*. Cryptologia, Taylor & Francis, 2017, 41 (5), p.6, Retrieved December 3, 2017 from http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1238422 <hal-01397035>.

[2] Colleen, *Why Teach a Cryptology Unit Study?* Retrieved December 3, 2017, from https://raisinglifelonglearners.com/why-teach-a-cryptology-unit-study/.

[3] Damico, Tony M. *A Brief History of Cryptography*, Vol. 1, No. 11, PG 1/1. Retrieved December 1, 2017, from http://www.inquiriesjournal.com/articles/1698/a-brief-history-of-cryptography.

[4] Danesi, Marchel. *Cryptograms and the Allure of Secret Codes*. Posted in https://www.psychologytoday.com/blog/brain-workout/201009/cryptograms-and-the-allure-secret-codes, on September 22nd, 2010. Retrieved December 2, 2017.

[5] Dushi, Gauri. *Notes on the Types of Education: Formal, Informal, Non-formal*. Retrieved December 2, 2017, from

http://www.preservearticles.com/2012010920241/notes-on-the-types-of-education-formal-informal-non-formal.html.
[6] Encyclopedia of Mental Disorders, *Standford-Binet Intelligence Scale*, Retrieved December 3, 2017 from http://www.minddisorders.com/Py-Z/Stanford-Binet-Intelligence-Scale.html.
[7] English, Oxford Living Dictionaries, *Child*. Retrieved December 2, 2017, from https://en.oxforddictionaries.com/definition/child.
[8] Enhancing Education, Retrieved December 2, 2017, from http://enhancinged.wgbh.org/started/what/formal.html.
[9] Johnson, George E. 1916. *Education through Recreation*. Philadelphia: The Survey Committee of the Cleveland Foundation. Retrieved December 3, 2017 from https://archive.org/stream/educationthrough00johnuoft#page/n5/mode/2up.
[10] Kautzer, Kim. *Building Writing Skills with Word Games and Puzzle*. Posted in https://writeshop.com/build-skills-puzzles-word-games/ on April 13, 2015. Retrieved December 3, 2017.
[11] Koblitz, Neal. 1997. *Cryptography as a Teaching Tool*. An article in Cryptologia, Vol.21, No. 4. Retrieved December 3, 2017, from https://sites.math.washington.edu/~koblitz/crlogia.html.
[12] Mead, George Herbert. *The Relation of Play to Education*, University Record 1, No. 8, (1896): 141-145. Retrieved December 3, 2017 from https://brocku.ca/MeadProject/Mead/pubs/Mead_1896.html
[13] Merriam-Webster Dictionary, Retrieved December 2, 2017, from https://www.merriam-webster.com/dictionary/education.
[14] Munir, Rinaldi. 2006. *Diktat Kuliah IF 2120: Matematika Diskrit*. Ed. 4. Bandung: Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.
[15] Myers, Pam. *Why Puzzles are Good for Your Child's Development*. Posted in https://childdevelopmentinfo.com/child-activities/why-puzzles-are-good-for-your-childs-development/#.WiQI2kqWY2z on November 2, 2011. Retrieved December 3, 2017.
[16] Spivey, Becky L. and Susie S. Loraine, M.A., CCC-SLP. 2010. *Puzzles—Toys...or Teaching Tools?* In "Super Duper Handy Handout" Number 245. Greenville: Super Duper Publications. Retrieved December 3, 2017 from https://www.superduperinc.com/handouts/pdf/245_Puzzles.pdf.
[17] Westman, Jack C., Victoria Costello. 2011. *The Complete Idiot's Guide to Child and Adolescent Psychology*. New York: Marie Butler-Knight. Retrieved December 3, 2017 from https://books.google.co.id/books?id=52mbbm4xKuIC&pg=PT241&dq=cryptography+child+psychology&hl=id&sa=X&ved=0ahUKEwju0vDouO7XAhWJpo8KHaVdCQIQ6AEIPjAD#v=onepage&q=cryptography%20child%20psychology&f=false.
*alphabetic ordered

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 3 Desember 2017

Ranindya Paramitha
13516006