TEACHING ENCRYPTION: A LEARNING THEORY APPROACH

A Paper
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Manu Kishore Bhogadi

In Partial Fulfillment of the Requirements
for the Degree of
MASTER OF SCIENCE

Major Department:
Computer Science

October 2010

Fargo, North Dakota

North Dakota State University
Graduate School

Title

TEACHING ENCRYPTION:

A LEARNING THEORY APPROACH

By

MANU KISHORE BHOGADI

The Supervisory Committee certifies that this ***disquisition*** complies with North Dakota State University's regulations and meets the accepted standards for the degree of

MASTER OF SCIENCE

ABSTRACT

Bhogadi, Manu Kishore, M.S., Department of Computer Science, College of Science and Mathematics, North Dakota State University, October 2010. Teaching Encryption: A Learning Theory Approach. Major Professor: Dr. Kendall E. Nygard.

Bloom's taxonomy for cognitive domain is an effective taxonomy for structured learning. The six levels in Bloom's taxonomy for cognitive domain are based on the levels of difficulty. This paper focuses on teaching communication security and encryption by applying Bloom's taxonomy in the creation of educational materials and assessments.

Delivering education material to the mobile phones is made possible with the advancement of mobile technologies, and the use of mobile technologies in teaching is gaining popularity because of its benefits. In this paper, delivering educational material to the mobile phones is experimented with by using a flash cards application for android based mobile phones.

Experiential learning is learning by doing, is active, motivating and enables learners to retain knowledge to a greater extent. This paper provides a tool to learn RSA public key cryptographic algorithm through experiential learning.

ACKNOWLEDGMENTS

I would like to thank my advisor, Dr. Kendall Nygard, for his support, guidance, and expertise. My sincere thanks to Dr. Hyunsook Do, Dr. Gursimran Walia and Dr. Sivapalan Gajan for serving on the committee.

I would also like to thank my parents, elder sister and elder brother. They were always supporting me and encouraging me with their best wishes.

Finally, I would like to thank my friends for their continuous encouragement and support.

TABLE OF CONTENTS

LIST OF TABLES

Table Page

LIST OF FIGURES

1. INTRODUCTION

1.1. Challenges in Learning

Learners face a wide variety of challenges when learning new concepts, one of which is the structure of their learning. It is difficult to learn complex concepts initially without the fundamental knowledge on which the concepts are based on. Also, the complexity of the learning is based on the amount of content the learners try to learn during the various stages of the learning, therefore, the complexity of learning depends on how the learners approach the concepts when they are learning. If the learners do not have prerequisite knowledge about the concepts they are learning, it is harder for them to learn. Often, learners go back and forth when trying to understand key or difficult concepts when they need a good understanding of underlying topics.

Without a structure, learners may end up spending too much time or losing focus on the actual concepts they want to learn. There are various activities which the learners need to do during the learning process, which may include remembering terms, understanding concepts, using concepts to gain a better perspective, and so on. Selection of these activities needs careful attention in order to teach efficiently. Most of the times, learners were asked just to reproduce the knowledge.

Another challenge most of the learners face is the extent to which they can focus. Unless there is framework or a model which guides the levels in understanding, it is hard to quantify the target level of understanding. In general, target level of understanding is defined with the help of a framework. The levels vary based on the framework which defines the learning theory.

1.2. Educational Taxonomies

Taxonomy is a classification system that is ordered in some way. Most of the educational taxonomies divide educational objectives into three domains: cognitive, affective and psychomotor [9]. Educational taxonomies advocate effective teaching based on observation of how learning happens. Educational taxonomies are helpful in setting up the learning objectives and ways to assess the attainment [9].

Learning taxonomies describe various stages in the learning process which will aid our understanding about the learning [6].

Learning taxonomies can be used in designing the objectives of a course. By mapping the stages in learning to the stages in the taxonomy, it is possible to quantify the target understanding level of the learners. Designing the curriculum objectives of a course depends on the learner's intended level of understanding, but not all the concepts require advanced understanding; some concepts just require basic understanding. With the help of the learning taxonomies, the levels of understanding can be defined and achieved efficiently. Thus, learning taxonomies is useful for both the teaching and learning purposes.

The stages in the learning taxonomies are used to describe the learners understanding levels. Different learners operate at different stages, even though they are all learning in the same class. Once the objectives are set with the help of learning taxonomies, they should be checked with the proper assessment. The assessments should be stage dependent, and one assessment technique, such as quiz, may not be used to determine whether learners can create something with the knowledge they posses. The assessment will determine whether the learners operate in a stage intended by the instructor. These assessments give the instructor a chance to revise the teaching style, educational content and curriculum objectives.

Learning taxonomies are widely used to describe the learning stages at which a learner is operating for a certain topic. For example, a learner may be capable of reciting by heart what recursion is, but not capable of implementing a recursive algorithm. An instructor may aim to have his or her learners learn a topic at a certain level in taxonomy.

Learning taxonomies can be introduced to the learners, which will help them understand the mapping between the taxonomy stages and the activities they are required to complete. By knowing which stage they are required to be operated at, they can be well prepared for that stage. For example, they can expect the level of questions they will be tested with and be prepared.

There are various learning taxonomies, instructional design strategies and theories developed to assist the creation of educational resources and the development of learning outcomes. The most widely used learning taxonomy is Bloom's taxonomy, as the ease of adapting Bloom's taxonomy made it popular and widely used.

1.3. Bloom's Taxonomy

Benjamin Bloom, an educational psychologist, found that 95% of the questions the learners are asked in their test require them to recall information, making them to think at the lowest possible levels [7]. Benjamin Bloom, who led a group of educational psychologists, identified three domains of educational activities:

- Cognitive: mental skills (knowledge)
- Affective: growth in feelings or emotional areas (Attitude)

- Psychomotor: manual or physical skills (Skills)

These are popularly known as Bloom's taxonomy of learning domains. In this paper, only the cognitive domain is required for teaching encryption and, hence, the designing of the course content is in accordance with the Bloom's taxonomy for cognitive domain. In the cognitive domain, knowledge and the development of intellectual skills are involved. The concept of Bloom's taxonomy is based on the levels of difficulties, where each level addresses different learning activities. These levels are dependent, meaning the lower level is a prerequisite for the higher level. The six categories in Bloom's taxonomy for cognitive domain are shown in Figure 1. The knowledge level is the lowest level and evaluation level is the highest level.

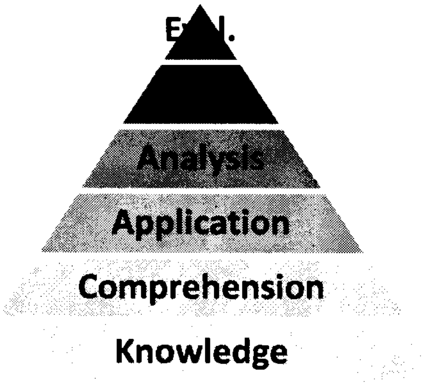


Figure 1. Bloom's taxonomy of cognitive domain

1.4. Revised Bloom's Taxonomy

A former student of Bloom's, Lorin Anderson, led a new group to update the original Bloom's taxonomy. The main purpose of revisiting Bloom's taxonomy, which was proposed in 1956, is to add relevance for students and teachers of the present time. The terms used for stages in the original Bloom's taxonomy is often confusing and results in overlapping stages. The group spent six years finalizing their work, which was published in 2001. Though the changes are minor, they are quite significant and occurred in three categories: terminology, structure and emphasis.

1.4.1. Terminology Changes

One of the most obvious differences is the change of category names from nouns to verbs. The new terms are defined as in the Table 1 and the difference is shown in Figure 2.

Table 1. Levels and cognitive processes adapted from [8]

Categories	**Cognitive Process**
Remember	**Retrieve relevant knowledge from long-term memory** **RECOGNIZING** (identifying) **RECALLING** (retrieving)
Understand	**Construct meaning from instructional messages, including oral, written, and graphic communication** **INTERPRETING** (clarifying, paraphrasing, representing, translating) **EXEMPLIFYING** (illustrating, instantiating) **CLASSIFYING** (categorizing, subsuming) **SUMMARIZING** (abstracting, generalizing) **INFERRING** (concluding, extrapolating, interpolating, predicting) **COMPARING** (contrasting, mapping, matching) **EXPLAINING** (constructing models)
Apply	**Carry out or use a procedure in a given situation** **EXECUTING** (carrying out) **IMPLEMENTING** (using)
Analyze	**Break material into its constituent parts and determine how the parts relate to one another and to an overall structure or purpose** **DIFFERENTIATING** (discriminating, distinguishing, focusing, selecting) **ORGANIZING** (finding coherence, integrating, outlining, parsing) **ATTRIBUTING** (deconstructing)
Evaluate	**Make judgments based on criteria and standards** **CHECKING** (coordinating, detecting, monitoring, testing **CRITIQUING** (judging)
Create	**Put elements together to form a coherent or functional whole; reorganize elements into a new pattern or structure** **GENERATING** (hypothesizing) **PLANNING** (designing) **PRODUCING** (constructing)

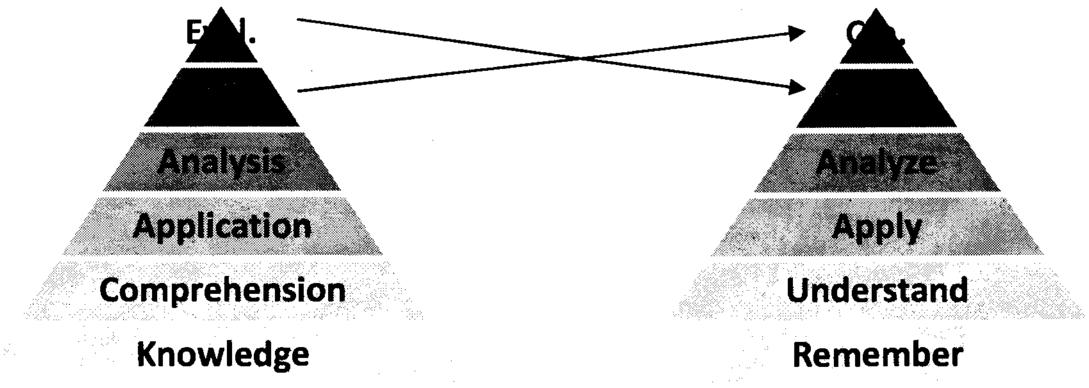


Figure 2. Comparison of original and revised Bloom's taxonomy

1.4.2. Structural Changes

Bloom's original taxonomy was a single-dimensional form. For example, the knowledge level has a number of activities such as arrange, define, label, list, order, recognize, recall, and repeat and so on. Knowledge is of different types and choosing between these activities is subjective, and mapping the activity for particular type of knowledge is often difficult. In revised Bloom's taxonomy, this was made easy by making taxonomy double-dimensional by classifying the knowledge dimension.

The Table 2 illustrates the structural changes in the revised Bloom's taxonomy. The knowledge dimension is made up of four types of knowledge which are factual knowledge, conceptual knowledge, procedural knowledge and meta-cognitive knowledge. Different concepts in a single subject may fall into different knowledge category. All the six levels have a different cognitive process for each knowledge category. It is easy to select the cognitive process based on the knowledge type the learner is dealing with. This was not straight forward in the original Bloom's taxonomy.

Table 2. Structural changes in revised Bloom's taxonomy adapted from [28]

The Knowledge Dimension	**The Cognitive Process Dimension**					
	Remember	Understand	Apply	Analyze	Evaluate	Create
Factual Knowledge	List	Summarize	Classify	Order	Rank	Combine
Conceptual Knowledge	Describe	Interpret	Experiment	Explain	Assess	Plan
Procedural Knowledge	Tabulate	Predict	Calculate	Differentiate	Conclude	Compose
Meta-Cognitive Knowledge	Appropriate Use	Execute	Construct	Achieve	Action	Actualize

1.4.3. Emphasis

The original Bloom's taxonomy was not intended for the use of various purposes, but was unexpectedly picked for numerous purposes such as teaching, learning, and research. The original Bloom's taxonomy was not addressing all those needs, but the revised taxonomy addressed this issue, and made it available for a much broader audience.

1.4.4. Lower Order Thinking and Higher Order Thinking Skills

The base three levels (Remember, Understand and Apply) are called Bloom's lower order thinking skills, while the top three levels (Analyze, Evaluate and create) are Bloom's higher order thinking skills. As the name suggests, higher order thinking skills goes beyond recalling facts or understanding concepts. In this paper, only the lower order thinking skills are targeted because of the intended duration of learning as well as understanding the concepts of communication security and encryption at the target level.

1.4.5. Levels in Revised Bloom's Taxonomy

There are six levels in the Revised Bloom's taxonomy. The six levels are explained as the following.

1.4.5.1. Remember Level

The Remember Level is the base level in the Bloom's taxonomy for cognitive domain. The main objective of this level is to recall information, which can be done through activities like recognizing, listing, describing, naming, retrieving or finding. These activities will vary based on the information and the topic for learning. Assessment can be done with the kind of exercises which target testing memorization. In this level, the knowledge is classified into 4 different types and, based on the knowledge type, certain assessment activities will be chosen. In this level, it is not necessary to have the understanding of the recalled information.

1.4.5.2. Understand Level

The Understand Level is based on the Remember Level. This level cannot be reached without completing the Remember level, and its main objective is to explain ideas or concepts related with the information learned in the Remember Level. The learning outcome of this level is one step beyond the Remember level. This level should be achieved in order to advance to next level in the Bloom's taxonomy. The assessment for this level can be done through activities like summarizing, interpreting, predicting or executing. Choosing between these activities depends on the type of knowledge.

1.4.5.3. Apply Level

The prerequisite for the Apply Level is the Understand Level. The main objective of this level is to use the information in another familiar situation. The assessment for this level can be done through activities like classifying, experimenting, calculating or constructing based on the knowledge type.

1.4.5.4. Analyze Level

The Analyze Level is the base of the higher order thinking skills, and its main objective is to break the information into parts in order to explore understanding and relationships. The assessment for this level can be done through activities like ordering, explaining, differentiating or achieving depending on the knowledge type.

1.4.5.5. Evaluate Level

The main objective of the Evaluate Level is to justify a decision or course of action. The assessment of this level can be done through activities like ranking, assessing, concluding or acting based on the knowledge type.

1.4.5.6. Create Level

The main objective of the Create Level is to generate new ideas, products or ways of viewing things. The assessment for this level can be done through activities like designing, constructing, planning, producing or inventing based on the knowledge type. This is the highest level to achieve in the Bloom's taxonomy.

1.5. Experiential Learning

"Research in Experiential learning has shown it is one of the effective methods for learning, especially when combine with other forms of instruction" [18]. The current paper focuses on introducing the key communication security and cryptography concepts and the RSA encryption algorithm.

While introducing the key terminology of communication security and cryptography is done through flashcards, handout and animated material, experiential learning for RSA public key encryption is done through executing the application in which the information is encrypted and decrypted. The experiential learning in the paper falls between an in-depth study of the RSA algorithm and the application of the RSA algorithm. Including laboratory kind of experience in the course is a great way to enhance the students learning experience. Most educators will present experiential learning in addition to the typical lecture model [19]. Perez-Hardy explains that the use of the laboratory approach in teaching network administration *"provides the best mechanism for making theory a reality for the student."* [19]. As Perez-hard states, labs should be *"designed to reinforce the theory covered in lecture"* [19]. Hazari explains one of the disadvantages of the lecture model [10]: *"Students are passive learners in this process, feedback from all students may not be evident, the lecture is delivered assuming average understanding and comprehension for the entire class thereby isolating learners who may be advanced or those needing remediation."* Hazari also explains that *"when used along with active learning techniques, the lecture becomes even more powerful in achieving instructional goals."*

1.6. Communication Security and Encryption

The following are the key concepts involved in the communication security and encryption which this paper focuses on:

- Message security issues
- Attacks and mechanisms
- Security attacks
- Types of cryptography
- Secret key encryption
- Public key encryption
- Digital signature
- Key exchange
- Requirements for public-key cryptography
- The RSA algorithm and its advantages and disadvantages

1.7. Problem Definition

The goal of this paper is to develop education content and assessments for the learners to teach the concepts of communication security and encryption efficiently.

Learners face difficulties in learning encryption. Difficulties include not having material focused just on the specified topics, not having activities which make learning efficient, and lacking a well defined target level of understanding.

1.8. Solution

The solution for teaching encryption constitutes applying the revised Bloom's taxonomy principles to create educational material and teaching through experiential learning. This paper focuses only on cognitive learning and does not address any other forms of learning.

1.8.1. Revised Bloom's Taxonomy

This paper focuses on both the teaching and learning aspects. Teaching aspects include the design and development of course content and mapping content to the revised Bloom's taxonomy. Learning aspects include the design and development of tools which will help learning.

The Apply Level in the revised Bloom's taxonomy is the target level for the educational content and assessments designed in this paper. . In this paper, the learners are expected to achieve only the lower order thinking skills of Bloom's taxonomy. In order to target each level in the revised Bloom's taxonomy, the traditional lecture model is divided into three parts:

1. Handout and Flash cards with terminology in communication security and encryption which helps the learners remember easily
2. Animated Material explaining the concepts in communication security and encryption which helps the learners to gain good understanding of the concepts.
3. Instructions to execute the tool for encrypting and decrypting using the RSA public key encryption algorithm

Teaching will be structured by dividing the lecture model into three parts. The assessments to test the learner's attainment will be two quizzes for the Remember Level and the Understand Level and a tool to execute for the Apply Level. These assessments will make learners focus on the current level and enhance the learning process by being structured.

1.8.2. Experiential Learning

A tool is provided to perform the generation of public and private keys, encryption and decryption tasks. This tool is designed for the experiential learning of the RSA public key encryption algorithm. By executing the tool successfully, the learners enhance their understanding of the RSA public key encryption algorithm they already learned in the Understand level. Without the understanding of the RSA public key encryption algorithm, solely executing this tool may not help the learner. Since the algorithm involves complex computations, the learners are not required to calculate those in order to learn about the algorithm; this tool is provided.

2. DESIGNING THE REMEMBER LEVEL

The Remember Level is the base level, or lowest level, in Bloom's taxonomy. The objective of this level is that the learners should be imparted with the procedural knowledge about the concepts involved in the communication security and encryption. Learners should be able to recognize or recall the terminology and key definitions in the communication security and encryption. This level often is ignored in the traditional way of teaching. The Table 3 shows the knowledge type and the cognitive process for the Remember Level.

Table 3. Knowledge type and cognitive process for the Remember Level

Knowledge type	Cognitive process for the Remember Level
Procedural knowledge	Recognizing and Recalling

2.1. Education Material

Since this is a first step in teaching, the educational material provided should act as good starting point, and the information should not overwhelm the learners. The material should be simple and should help learners achieve the objective of this level by being easy to remember the terminology and key terms. Educational material designed for this level is based on the assumption that the learners of the communication security and encryption do not necessarily have any previous knowledge of the security or encryption concepts.

2.1.1. Terminology and Definitions Handout

For this level, the material will have just the definitions of the important terms. This will introduce the actual terminology of the communication security and cryptography and is little different than the conventional way of teaching where the introduction of the concepts will be comprehensive. By separating the definitions and terminology from the rest of the teaching material, it will be easy for the learner to start learning no matter how complex the concepts are. In this level the users are expected to remember the concepts, so the complexity of learning will not be reflected in this level.

2.1.2. Flash Cards

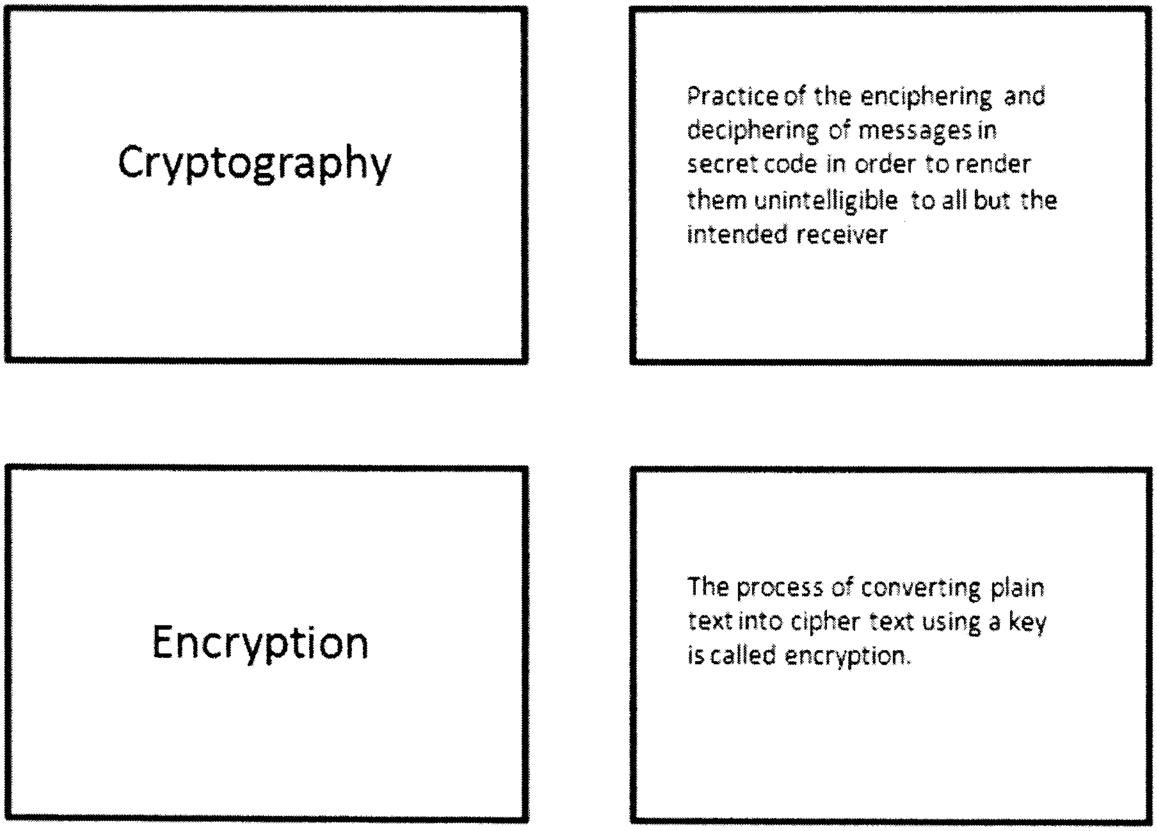
Apart from the handout, flash cards about the communication security and encryption will help users remember concepts. A flash card is a small card with some information on it and is used as a tool to help remember information. They are useful specially in remembering words and their meanings, definitions, facts, or mathematical formulas. They are based on a spaced learning technique and can have anything which can be used learn by question and answer format. Having too much of information on a flash card may not serve their purpose but can be made interesting by choosing the interesting color,, size, or flash card material. Having appropriate pictures along with the information will help students remember more efficiently. Flash cards with information on one side and a question about that information on the other side will have an added advantage and can be used as a self test tool.

The effectiveness of the flash cards would depends on the individual use and elements such as how one reacts to errors, frequency of use, information about related items and the creation of the flash cards [12]. Advantages of the flash cards are:

- They are easy to carry.
- They can be used almost anywhere.

- Creating Flash Cards is easy
- Changing the order of the flash cards is easy

The same terminology and definitions provided in the handout can be delivered in the form of flash cards. All the advantages of the flashcards can be gained by providing the educational material in the form of flash cards for this Remember Level. In the below Figure 3, two flash cards are presented side by side. The front side of the first flash card has just the word "Cryptography" and the back side of the card has its definition next to it.



Cryptography

Practice of the enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver

Encryption

The process of converting plain text into cipher text using a key is called encryption.

Figure 3. Front and back side of flash cards

The “Encryption” flash card is the same. The layout will look different when printing the actual flash cards as each card is a piece of paper that has the word on its front side and the definition on the back side.

2.1.2.1. Flash Cards for Mobile Phones

The flash cards can be provided in an electronic format and made available to the learners in the form of a mobile application. The design goal of the flash cards and the mobile phone usage will make the flash cards application for the mobile phones apt. In this paper, an effort is made to explore the mobile phone space available for delivering educational material in the form of a mobile application. An open source android application is provided for the same purpose.

2.1.2.2. Android Development

Android is an operating system based on Linux with a Java programming interface. It provides tools, e.g. a compiler, debugger and a device emulator, as well as its own Java Virtual machine (Dalvik Virtual Machine - DVM). Android is created by the Open Handset Alliance which is led by Google.

Android uses a special Java virtual machine (Dalvik), which is based on the Apache Harmony Java implementation. Dalvik uses special bytecode. Therefore, a standard Java byte code cannot be run on Android. Android provides a tool, "dx" which allows the conversion of Java Class files into "dex" (Dalvik Executable) files. Android applications are then packed into an .apk (Android Package) file.

Android supports 2-D and 3-D graphics using the OpenGL libraries and supports data storage in a SQLLite database. For development, Google provides the Android

Development Tools (ADT) for Eclipse in order to develop Android applications. Every Android application runs in its own process and is isolated from other running applications. Therefore, one misbehaving application cannot harm other Android applications.

2.1.2.3. Android Software Layers

The software layers in android are shown in the Figure 4.

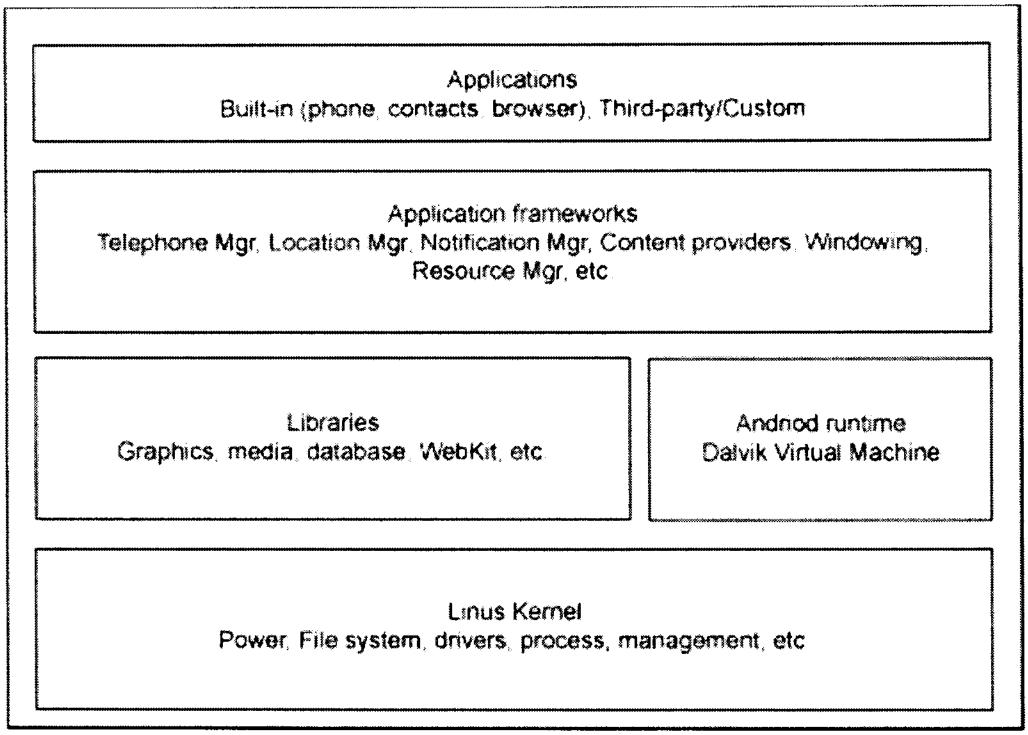

Applications
Built-in (phone, contacts, browser), Third-party/Custom
Application frameworks
Telephone Mgr, Location Mgr, Notification Mgr, Content providers, Windowing, Resource Mgr, etc
Libraries
Graphics, media, database, WebKit, etc
Android runtime
Dalvik Virtual Machine
Linus Kernel
Power, File system, drivers, process, management, etc

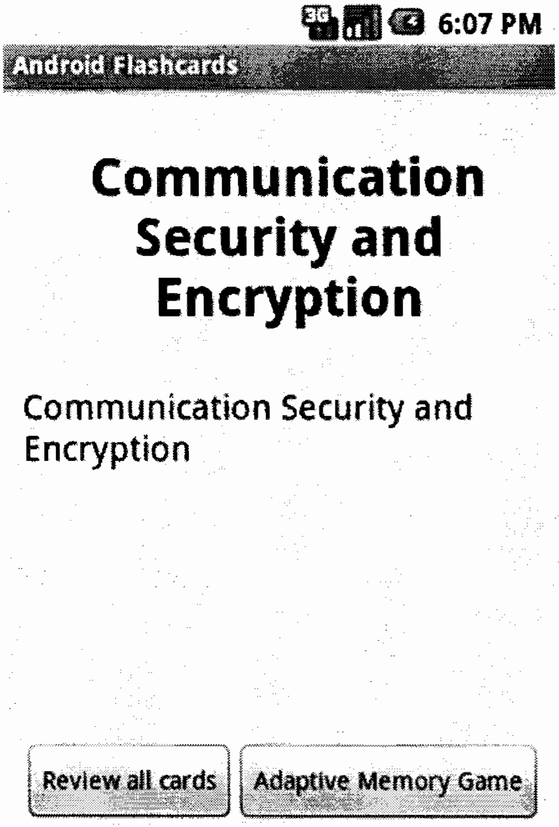
Figure 4. Software layers in android [11]

2.1.2.4. Android Flashcards

Android Flashcards is an open source application developed on an android platform and is used for learning through flash cards. This application was developed by Nick Lanham [3]. This application is simple in terms of creating new flash cards and accessing them. The flash cards are grouped into lessons.

This application can work in two modes as shown in the Figure 5. The two modes are

1. Simple card review mode
2. Adaptive memory game



Communication Security and Encryption

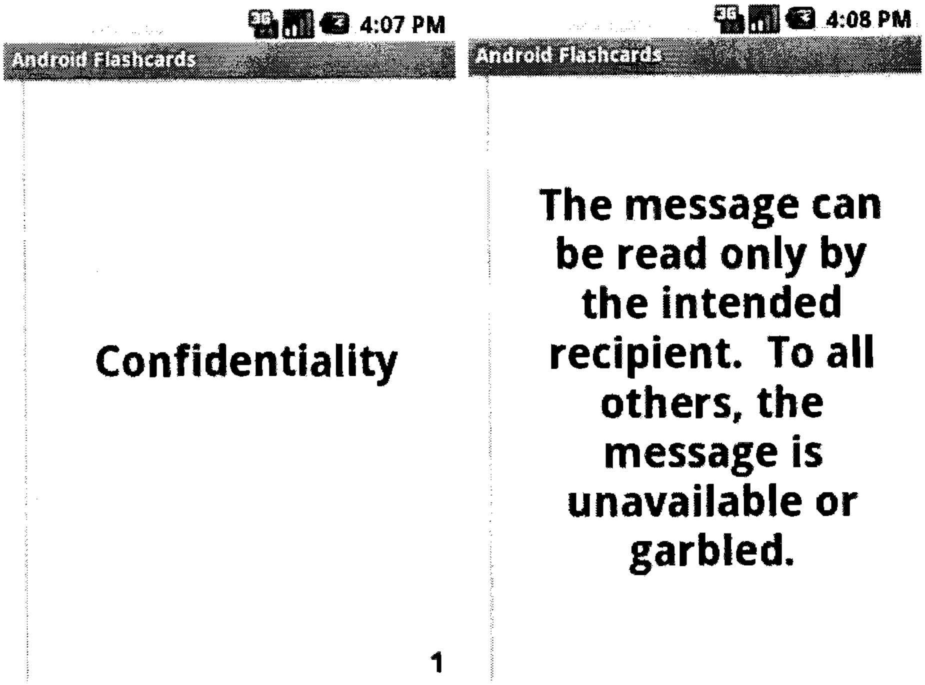
Communication Security and Encryption

Figure 5. Modes available in android flashcards

2.1.2.4.1. Simple Card Review Mode

In the Simple Card Review Mode, all the flash cards of a particular lesson can be reviewed in a sequential manner by swiping the screen forward or backward. Users can jump to a particular card by using the card number. A flash card should be tapped to view the back side of it. This mode is useful when reviewing the flash cards for the first time.

As shown in the Figure 6, the front side of a flash card has a keyword and the back side of the flash card has the definition or explanation for the keyword.



Confidentiality

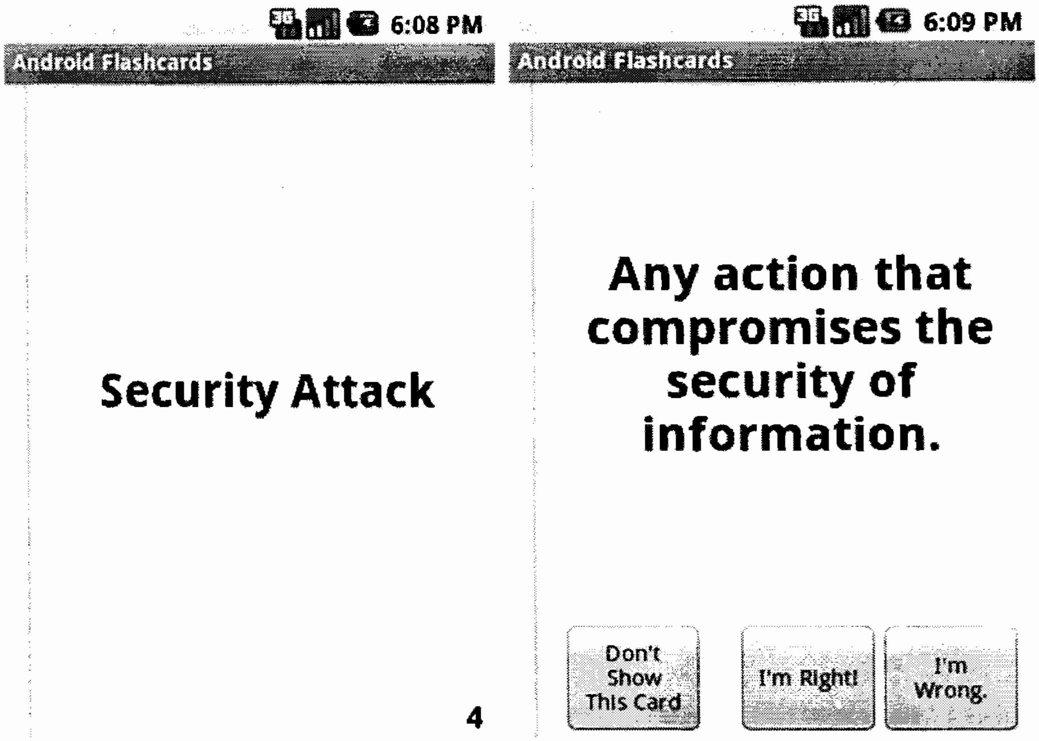
1

The message can be read only by the intended recipient. To all others, the message is unavailable or garbled.

Figure 6. Front and back sides of a flash card in review all cards mode

2.1.2.4.2. Adaptive Memory Game

The Adaptive Memory Game Mode acts as a quiz. In this mode, a random flash card can be reviewed and options can be selected such as "Don't show this card", "I'm right", "I'm wrong." Selecting these options will determine the randomness of the flash cards. The flash cards which are selected for "I'm wrong" have the high probability for repetition. Thus, the cards answered incorrectly will be shown more frequently, which helps learning. The cards which were answered correctly are shown less frequently. As shown in the Figure 7, the adaptive memory game mode has three buttons on the screen for easy navigation.



Security Attack

4

Any action that compromises the security of information.

Figure 7. Adaptive memory game mode

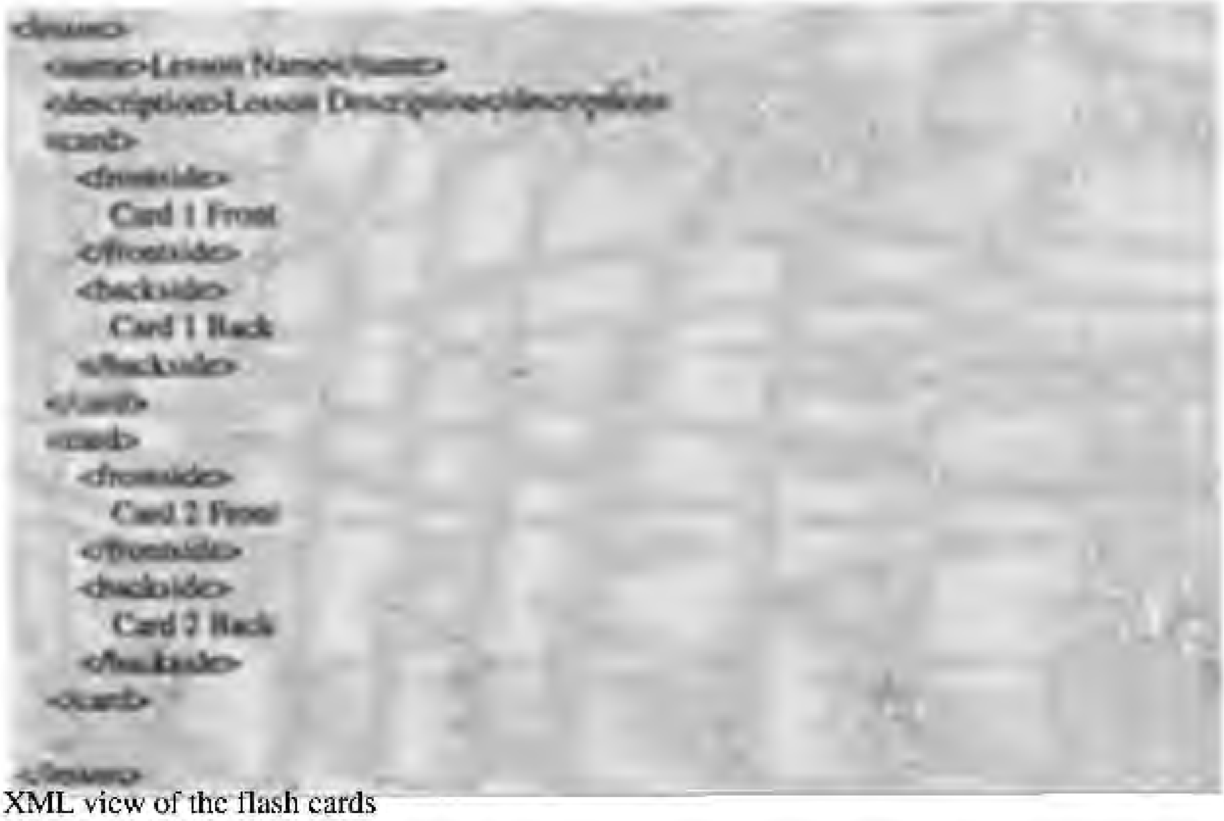
2.1.2.4.3. Adding Flash Cards

Flash cards for the mobile application are stored in the flashcards folder on the SD card and can be added in three ways:

1. Using XML file
2. Using CSV file
3. Using Spread Sheet

Flash cards can be added or deleted just by adding or deleting the information from the file. In xml view, flash cards are the "card" nodes: children of the node lesson. New flash card can be added just by adding the node "card" and entering the front and back sides of the card. A flash card can be deleted by deleting the particular "card" node.

In CSV view, each flash card is a line in the file. A flash card can be added by just inserting a new row and entering the information from the front and back sides, separated by the comma.

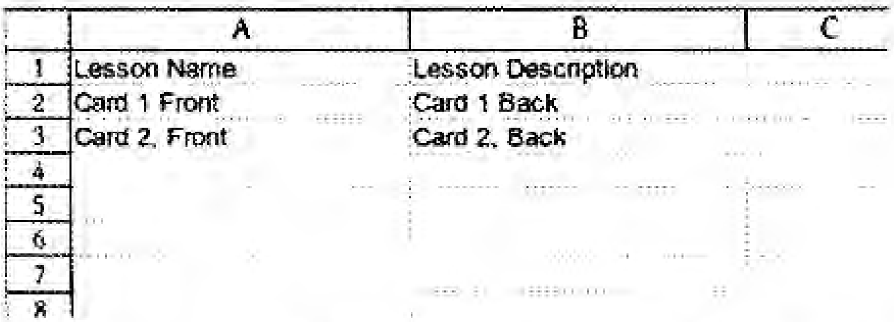


```
<[illegible]>
  <name>Lesson Name</name>
  <description>Lesson Description</description>
  <card>
    <frontside>
      Card 1 Front
    </frontside>
    <backside>
      Card 1 Back
    </backside>
  </card>
  <card>
    <frontside>
      Card 2 Front
    </frontside>
    <backside>
      Card 2 Back
    </backside>
  </card>

</[illegible]>
```

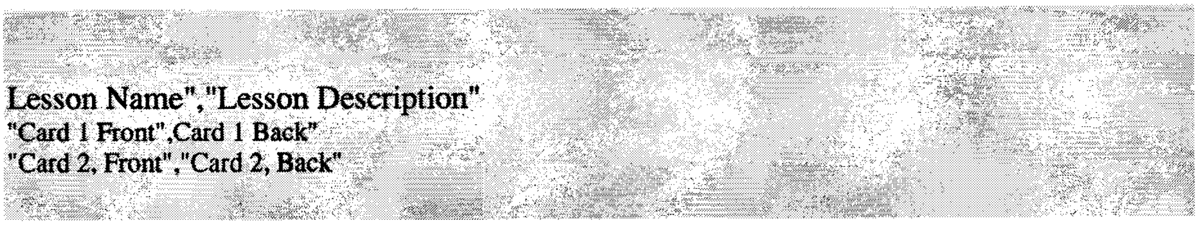
XML view of the flash cards

In spread sheet view, each flash card is presented in a line, and the front and back sides of the flash card are in each cell as shown in the Figure 8.



	A	B	C
1	Lesson Name	Lesson Description	
2	Card 1 Front	Card 1 Back	
3	Card 2, Front	Card 2, Back	
4			
5			
6			
7			
8			

Figure 8. Spread sheet view of the flash cards



```
Lesson Name","Lesson Description"
"Card 1 Front",Card 1 Back"
"Card 2, Front","Card 2, Back"
```

CSV view of the flash cards

2.2. Handout, Flashcards and the Remember Level

Providing the definitions about the security and cryptography information, which is free from comprehensive explanations, will ease the learners' ability to recall procedural knowledge. Providing the flash card tool as a means to learn content through review will enable learners to effectively recall information in testing. Having a quiz that expects the learner only to recall the information, but not necessarily understand, confines the learning to just the Remember Level in Bloom's taxonomy. Thus, the material provided for the Remember Level will fit into Bloom's taxonomy both from the teaching and learning perspectives.

2.3. Assessment of the Remember Level

Assessing learners in the Remember Level can be done with the help of a quiz. A quiz can be mapped for more than one level in the lower levels of Bloom's taxonomy, but the objective of the questions in the quiz will depend on which level of the Bloom's taxonomy the quiz is for. The objective of assessing the Remember Level is to find out whether the learner can recollect the terminology he/she learned with the help of the flash cards or the handout.

A mobile phone application in this level can also be used as self test tool for the learners while learning.

The quiz will focus on the activities of remembering, so the questions in the quiz should reflect this by asking “What” questions, instead of “why” questions. By answering the questions in the quiz, the learner needs only to recollect or recognize the information, and the learner need not reason or relate the information learned in the Remember Level.

2.3.1. Auto Grading

During the design of the quiz, an effort was made to reduce the effort of the quiz grader in the Remember Level. Auto grading will make use of some system by automatically evaluating the answers submitted by the users with the stored answers to the questions, requiring no effort from the grader. True or false questions are best suitable for the auto grading and having a percentage of these questions in the quiz will reduce the effort needed by the grader to evaluate the answers

3. DESIGNING THE UNDERSTAND LEVEL

The Understand Level involves explanation about the terminology and key concepts in the communication security and encryption and assessment in order to test the attainment of the learner. This level is based on the Remember Level. If the Remember Level is skipped by starting with the Understand Level, the structured learning advised by Bloom's taxonomy will breakdown. The Table 4 shows the knowledge type and the cognitive process for the Understand Level.

Table 4. Knowledge type and cognitive process for the Understand Level

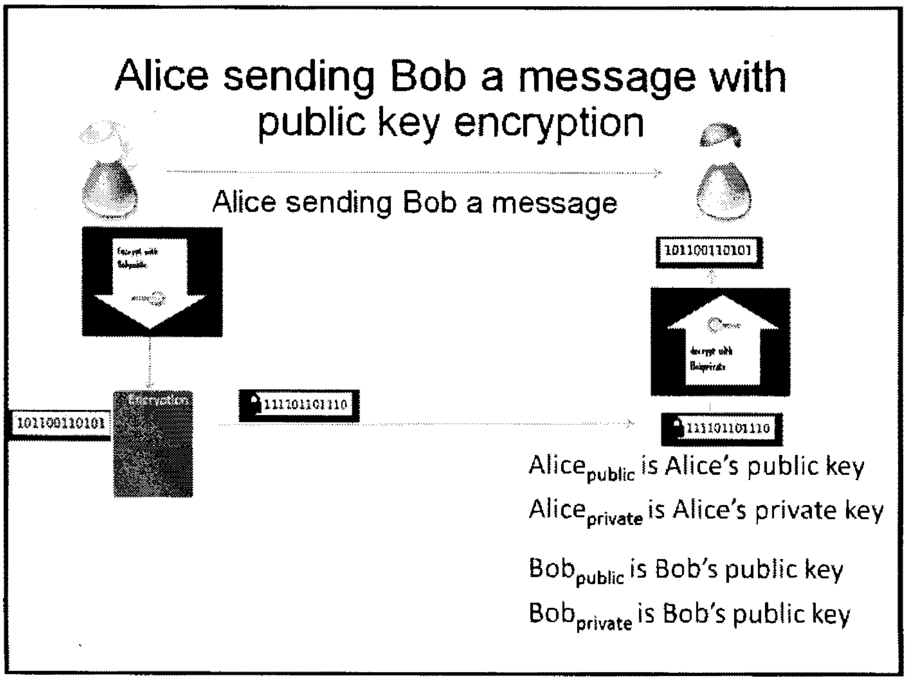
Knowledge type	Cognitive process for the Understand Level
Procedural knowledge	Exemplifying

3.1. Education Material

Education material provided in this level should help the learners understand the key concepts involved in the communication security and encryption. The explanation should go beyond the definitions and connect the learner and education material. The order in which the concepts are introduced and explained should ease the difficulty of understanding the concepts. With the help of the education material presented in this level, the learners should be able to explain the concepts in their own words. One of the key objectives in creating the education material is not to create material which does not exist, but to select the existing material, thereby helping learners understand the concepts. The emphasis here is to select the appropriate educational activities and the education material which makes the learning efficient.

3.1.1. PowerPoint Slides

Microsoft PowerPoint has been used extensively in the educational field and can accommodate the various requirements of presentations and educational material. The ease with which Microsoft PowerPoint can be used and prepared is also an important factor for its extensive use. Various elements like simple animations, graphics, sounds and text effects can be easily incorporated into the slides. The slides for communication security and encryption will have images that represent various elements. A picture of a key will represent a private key or public key. A picture of a person will represent the sender or receiver. These representations will help the learners understand the concepts. The slides provided are not comprehensive and thus they do not have extensive information about the concepts. The material covered in the slides will help the user to achieve the basic understanding of the concepts. The Figure 9 shows a slide with encryption and decryption.



Alice sending Bob a message with public key encryption

Alice$_{\text{public}}$ is Alice's public key

Alice$_{\text{private}}$ is Alice's private key

Bob$_{\text{public}}$ is Bob's public key

Bob$_{\text{private}}$ is Bob's public key

Figure 9. Slide showing encryption and decryption

3.1.2. Animated Material

"The multimedia effect refers to the finding that students learn more deeply from a multimedia explanation presented in words and pictures than in words alone." [16]

In addition to the PowerPoint slides, an animated version of the material covered in the PowerPoint slides is provided. The animations will help the learners understand the information about the cryptography and the public key encryption better. The animations may symbolize real world scenarios, and learners can navigate the topics and play the animations in any order. Learners can also stop an animation at a particular slide if they need more time to understand that particular topic, which allows the learners to feel in control of their learning. This is one of the implicit benefits of creating educational material that is learner interactive. In a classroom setting, a learner may not feel he is in control of learning since he has to adjust to the speed of the instructor.

3.1.2.1. Adobe Flash

Adobe flash is a multimedia platform used to add animation, video and interactivity to web pages. More recently, it has been positioned as a tool for "Rich Internet Applications". Adobe Flash is used extensively in developing Rich Internet Applications for websites. It is available as a free download from the adobe and installed in 98% of computers in the US. Some of the advantages for selecting flash for the development of animation in this paper are·

- Users can use the application from any web browser on any operating system
- Installation size is small
- It has richer user-interface than traditional html

3.1.2.2. Transmission of Message from the Sender to the Receiver

The transmission of data from the sender to the receiver (a sample scenario) is shown using the animation. The data starts at the sender, travels through the network, and reaches the receiver. Showing this information through animation eases the learners' understanding of the direction of the messages, where they originated, and where they ended within a short time. The learner has to figure out all this information through material or a normal PowerPoint slide. The Figure 10 and the Figure 11 shows a snapshot of the animation for the normal flow of information and public encryption rescpectively.

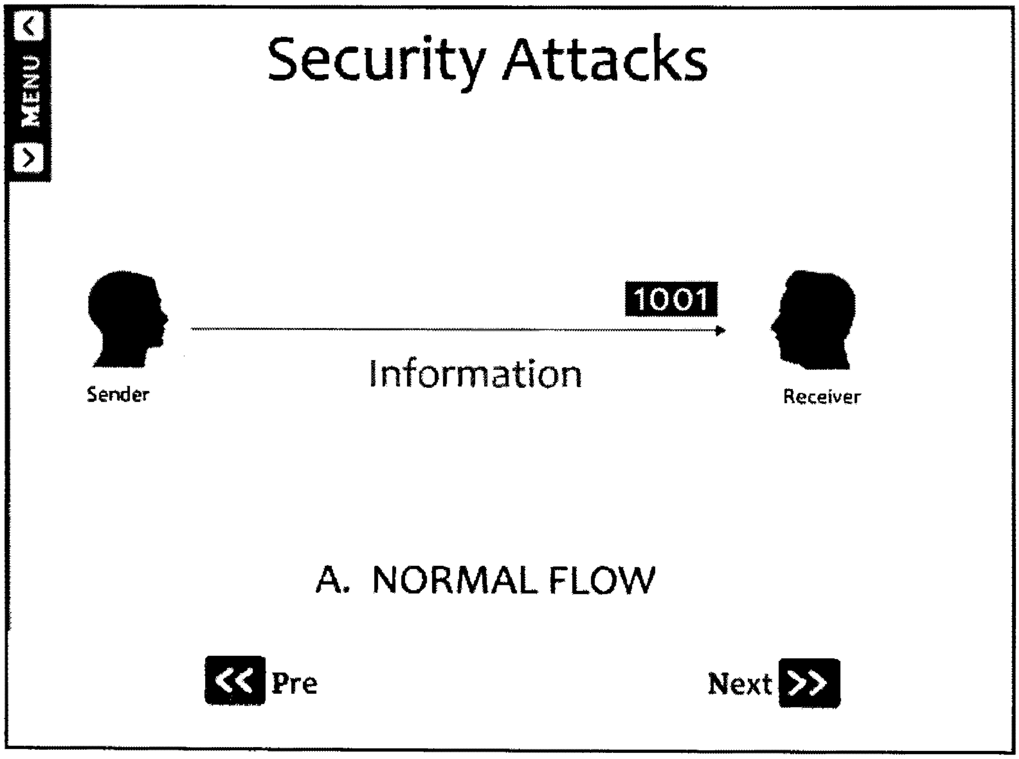


Figure 10. Animation showing the normal flow of information

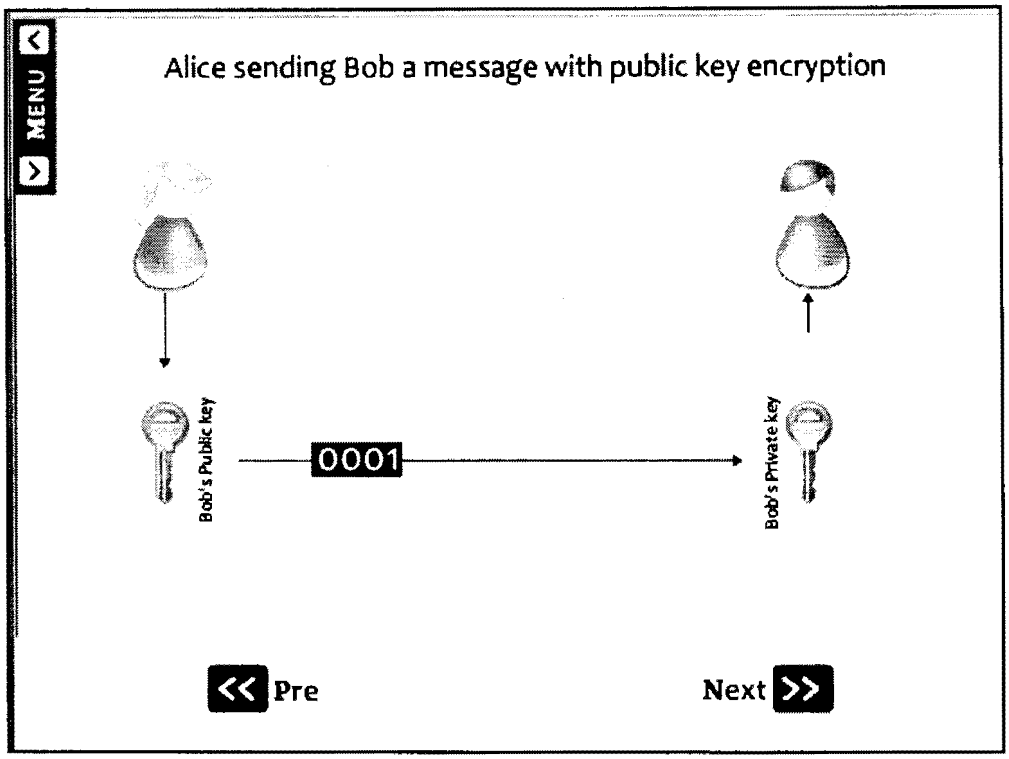


Figure 11. Animation showing Alice sending Bob a message

3.2. Animated Material and the Understand Level

Providing animated material in this level will result in the effective explanation of concepts involved in the communication security and encryption. Learners can relate to the concepts more easily through graphics with the procedural knowledge they learned in the Remember Level. Though the material provided is not comprehensive, it will be useful in understanding the key concepts.

3.3. Assessment of the Understand Level

A quiz can help to assess the Understand Level and will focus on the activities of understanding. Questions concerning the brief outline of the public key encryption will require more than just an ability to recall the information. The learner needs to understand the process in order to express it in his/her own words. The purpose of the quiz is to assess the understanding of the learner by creating the quiz with certain types of questions. Having a quiz focused only on testing the learners' understanding of the concepts will help find the student attainment up to the Understand Level, but not beyond that.

3.3.1. Auto Grading

Similar to the Remember Level, an effort is made to make some percentage of questions in the quiz that can be auto graded. Questions like calculating the key values, asking whether a number is prime number or not will be suitable for auto grading.

4. DESIGNING THE APPLY LEVEL

The Understand Level acts as the foundation level for the Apply Level. After reaching an understanding with the encryption concepts, learners can reinforce the RSA public key encryption algorithm they learned in the Understand Level by executing the provided tool. The Table 5 shows the knowledge type and the cognitive process for the Apply Level.

Table 5. Knowledge type and cognitive process for the Apply Level

Knowledge type	Cognitive process for the Apply Level
Procedural knowledge	Executing

4.1. Education Material

A tool is provided for this level in which the learner can encrypt plain text and decrypt cipher text with RSA public key encryption.

4.1.1. RSA Public Key Encryption Tool

In this application level, learners are required to execute the RSA public key encryption tool to gain better understanding of the RSA public key encryption algorithm. Though the learners are not required to study the arithmetic behind the RSA public key encryption, they need to understand the idea behind the algorithm. Learners can better understand the algorithm when they can actually generate the keys using the algorithm and perform encryption and decryption functionalities. Since generating the prime numbers and calculating the modular arithmetic would be time consuming and complex, those things can be automated and calculated by the tool. Allowing the learners to perform the complex arithmetic calculations involved in the RSA algorithm would defy the objective of teaching the RSA public encryption algorithm in this course. Without the tool, the learners would end up spending most of the lab time performing calculations. As the range of the prime numbers increase, the calculations involved in the algorithm would become extremely difficult to calculate. To keep learners focused on learning how the algorithm works, calculations can be delegated to the tool, which can generate random prime numbers, calculate private key, public keys, perform encryption and decryption.

Instructions on how to execute this tool are provided to the learners. By mapping the actual steps in the algorithm to the steps required to generate the keys and perform encryption and decryption, learners will have a working version of the algorithm.

An overview of the technologies used in creating the RSA public encryption tool is described below.

4.1.1.1. C# and Windows Forms Application

C# language is used to program the windows application. The target framework used for the application is .NET framework 3.5. Choosing C# language as a choice for the tool helps to achieve the advantages of the .NET framework such as language portability, easy application development and maintenance, consistent programming model, security, and so on.

A Windows form application is a typical desktop application. A Windows Forms application is an event-driven application supported by Microsoft's .NET Framework. Windows desktop application is chosen over the web application because the learners need not connect to internet when working with the tool.

4.1.1.2. GMP and BigInt

Additional libraries, other than the programming framework, are needed to support and deal with large numbers. . Currently, the biggest range that the .NET framework can support is 0 through +/-79,228,162,514,264,337,593,543,950,335 for decimal data type, which is 16 bytes long. In cryptography, this range is not adequate for most of the operations. There is a need for additional libraries which support arithmetic operations on big numbers and are fast; one such library is GMP.

GMP is a free library for arbitrary precision arithmetic that operates on signed integers, rational number and floating point numbers. Though there are no limitations to the size of the numbers imposed by the GMP, the limitations to the numbers and the operations are imposed by the underlying system on which they run. System features like memory and processor speed may impose limitations on the numbers and the operations.

The main target applications for GMP are cryptography applications and research, Internet security applications, algebra systems, computational algebra research, etc. GMP is faster than any other bignum library.

The several categories of functions in GMP are High-level signed integer arithmetic functions, High-level rational arithmetic functions, High-level floating-point arithmetic functions, etc.

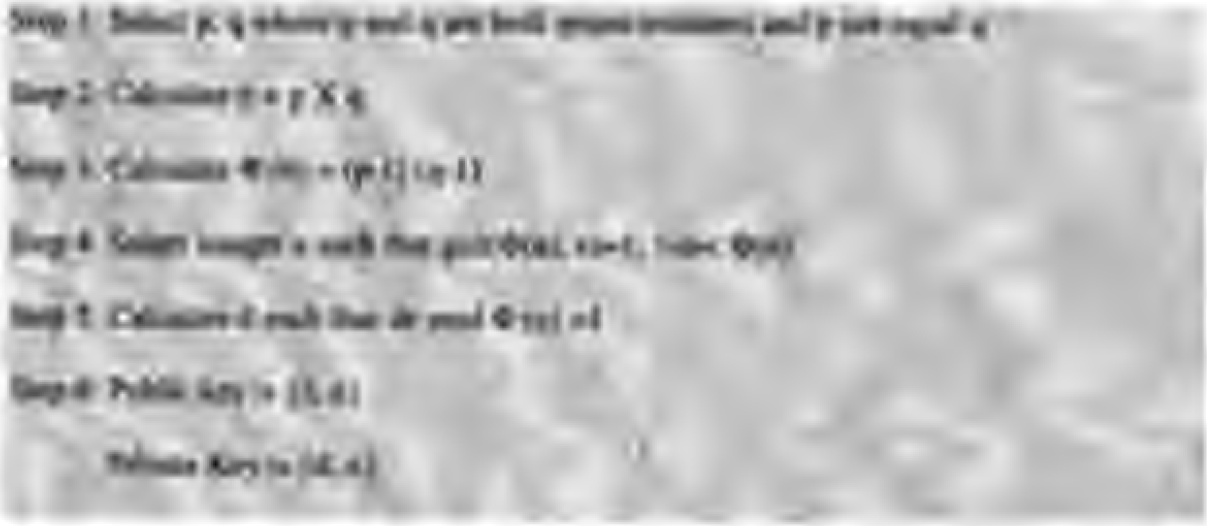
All these functions are based on C++ interfaces, and a .NET wrapper, the C# BigInt, is needed for these functions in order to use those in C#. This wrapper just provides a mechanism to interact with the C++ functions from the C# language. By having this wrapper, the calls to the GMP functions can be made as the calls to any other function in .NET.

4.1.1.3. RSA Public Key Encryption Algorithm

The RSA Algorithm is a public key encryption algorithm named after Rivest, Shamir and Adleman, who first publicly described it. The RSA algorithm is a widely used encryption algorithm and can be used for both the encryption and digital signing. The strength of the algorithm comes from computational difficulty of factoring large numbers. The major three steps involved in the algorithm are key generation, encrypting and decrypting.

4.1.1.3.1. Key Generation

The following are the steps involved in generating the public key and private key:



Step 1: Select p, q where p and q are both prime numbers and p not equal q

Step 2: Calculate n = p X q

Step 3: Calculate Φ(n) = (p-1) (q-1)

Step 4: Select integer e such that gcd(Φ(n), e)=1, 1<e< Φ(n)

Step 5: Calculate d such that de mod Φ(n) =1

Step 6: Public Key is {e, n}

Private Key is {d, n}

To send and receive messages in the encrypted format, a pair of keys (public key and private key) needs to be generated by both the sender and the recipient. Public key is meant for sharing and private key is kept secret. Both the sender and receiver should not exchange the private keys.

4.1.1.3.2. Encryption

Once the public key and private key of the recipient are generated, the public key can be published. The sender can encrypt the plain text with the public key and send it to the recipient.

Cipher text is calculated using the following formula:

m is the positive integer which represents the plaintext message

{n, e} is the recipient's public key

Cipher text $c=m^{e} \bmod n$

The cipher text c will be sent to the recipient.

4.1.1.3.3. Decryption

Once the cipher text c is received by the recipient, it can be decrypted using the recipient's private key in order to view the actual message m.

The plain text is calculated using the following formula:

{d, e} is the private key of the recipient

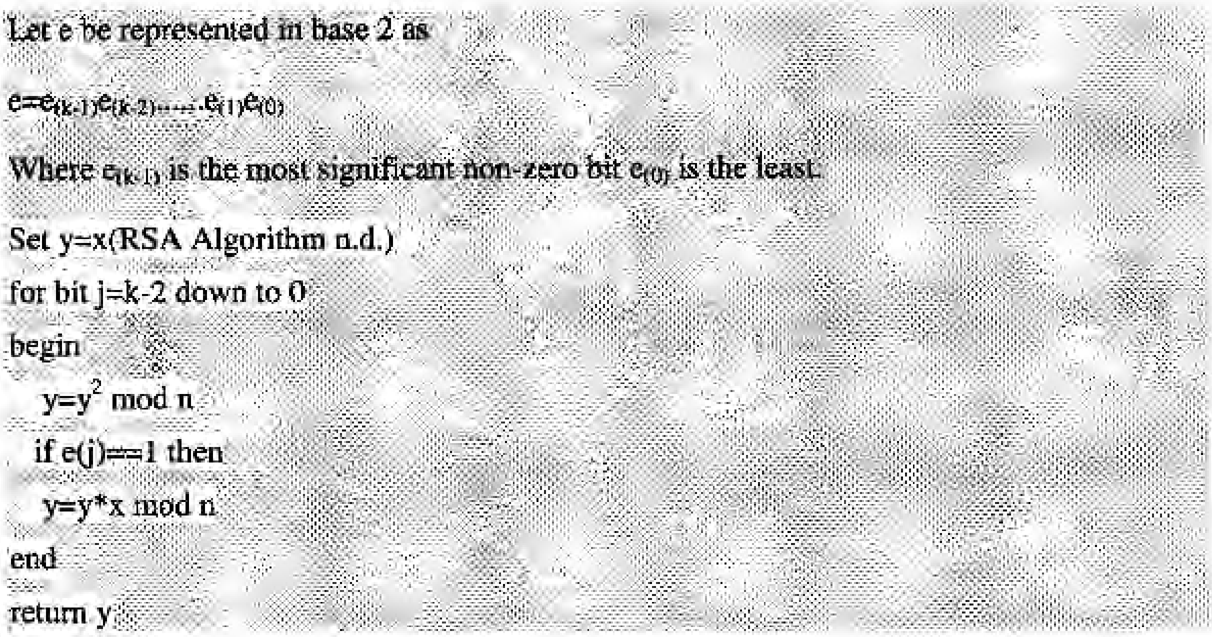
Plain text $m= c^{d} \bmod n$

4.1.1.4. Algorithm to Calculate Modular Exponential Values

Calculating the modular exponential value involved in the RSA public key algorithm using traditional methods is very expensive. This can be solved using the below algorithm, where exponential value is represented in binary format and is multiplied and squared based on the binary bits.

Algorithm

To solve $y= x^{e} \bmod n$



Let e be represented in base 2 as

$e=e_{(k-1)}e_{(k-2)}.....e_{(1)}e_{(0)}$

Where $e_{(k-1)}$ is the most significant non-zero bit $e_{(0)}$ is the least.

```
Set y=x(RSA Algorithm n.d.)
for bit j=k-2 down to 0
begin
   y=y^2 mod n
  if e(j)==1 then
   y=y*x mod n
end
return y
```

Example: calculating x for $x=5^5$ mod 5

Binary equivalent of 5 = 101

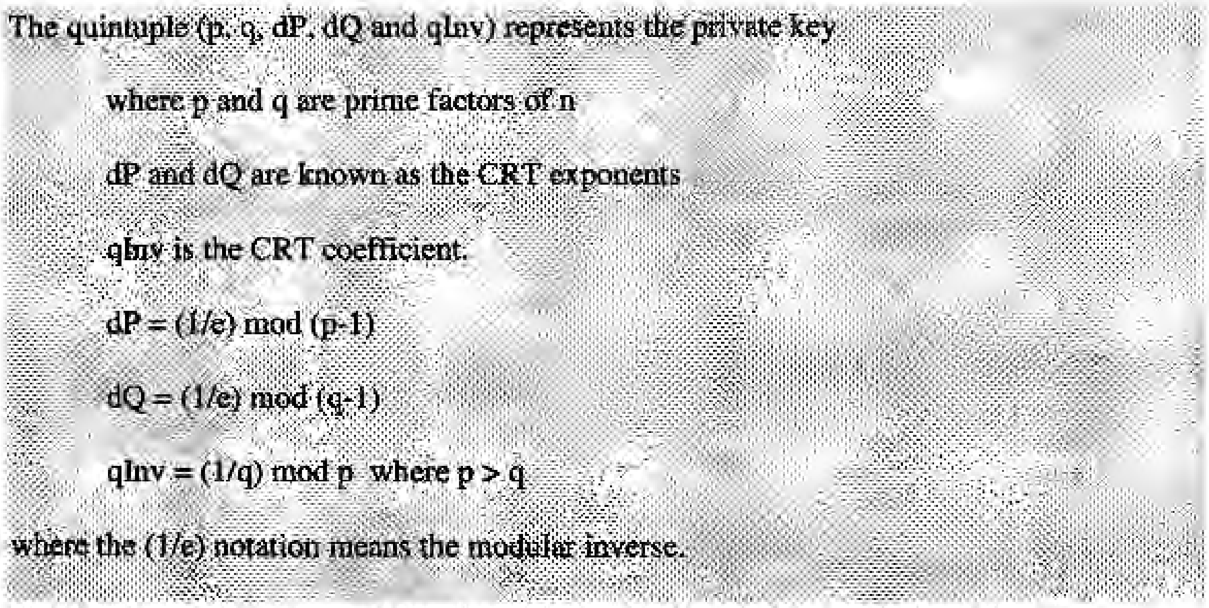
```
y=5
for j = [illegible]
j = [illegible]
y = [illegible] mod 5 = [illegible] mod 5 = [illegible]
j = [illegible]
y = [illegible] mod 5 = [illegible] mod 5 = [illegible]
y = [illegible] mod 5 = [illegible]
return y
```

Using the above method, the maximum number involved in the calculating 5^5 mod 5 is 25

4.1.1.5. Chinese Remainder Theorem

Calculating Plain text m= c ^{d} mod n is very expensive since c value is usually large. An alternate way not to calculate this is to represent the private key in order to perform simpler calculations using Chinese Remainder Theorem.

The private key in the RSA public key encryption can be represented as a quintuple using Chinese Remainder Theorem (CRT).



The quintuple (p, q, dP, dQ and qInv) represents the private key

where p and q are prime factors of n

dP and dQ are known as the CRT exponents

qInv is the CRT coefficient.

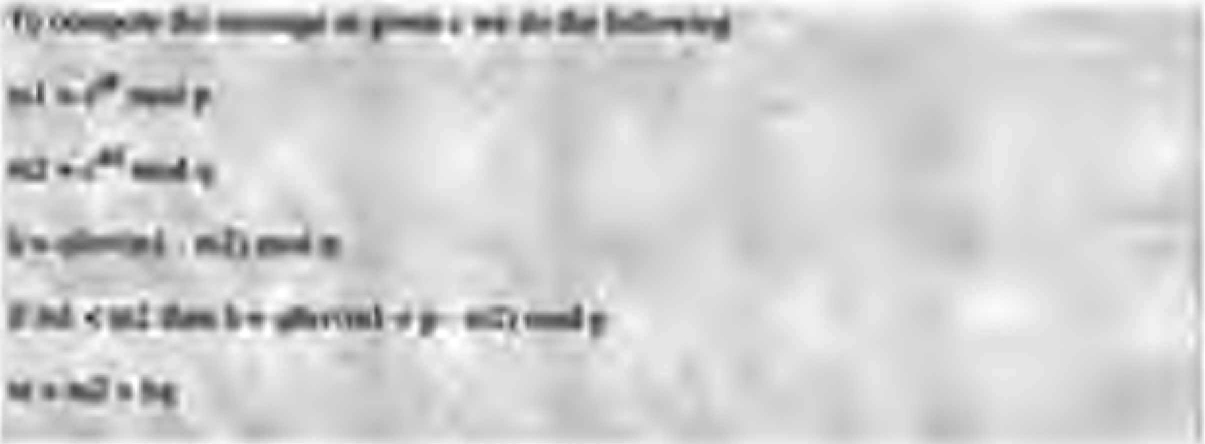
dP = (1/e) mod (p-1)

dQ = (1/e) mod (q-1)

qInv = (1/q) mod p where p > q

where the (1/e) notation means the modular inverse.

These values are pre-computed and saved along with p and q as the private key.



To compute the message m given c we do the following

$m1 = c^{dP} \bmod p$

$m2 = c^{dQ} \bmod q$

$h = qInv(m1 - m2) \bmod p$

if $m1 < m2$ then $h = qInv(m1 + p - m2) \bmod p$

$m = m2 + hq$

The decryption using CRT method is four times faster than calculating $m=c^d$ mod n.

4.1.1.6. Class Diagrams

The Figure 12 shows the overview of the classes in the RSA public encryption tool and the Figure 13 shows the RSA public class.

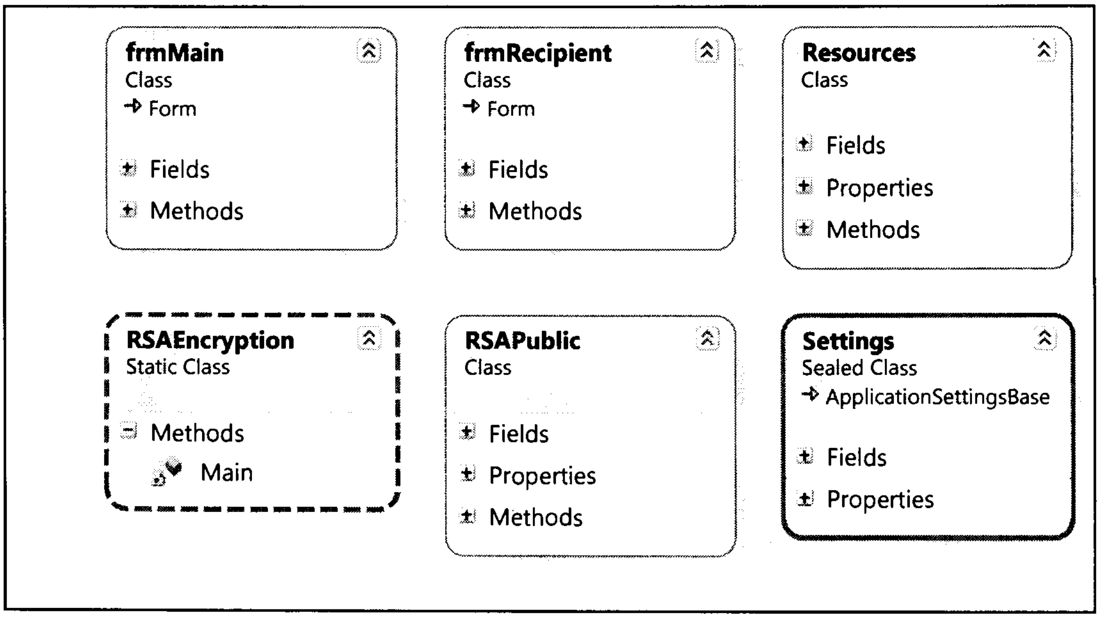


Figure 12. Class diagrams in RSA public encryption tool

4.1.1.6.1. RSA Public

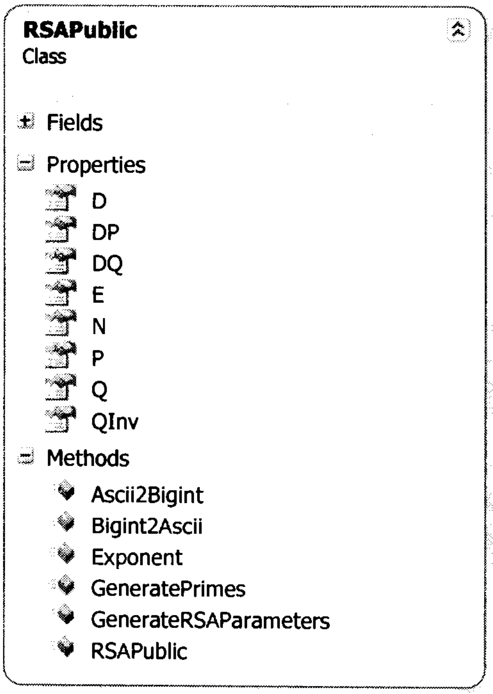
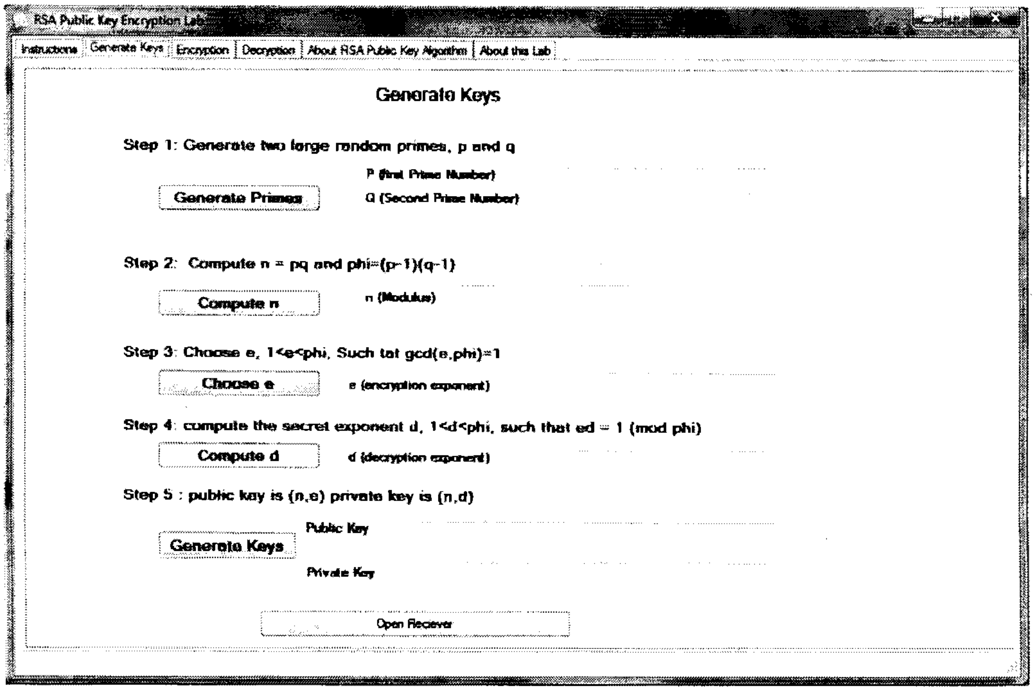


Figure 13. Class diagram of RSA public

All the complex calculations required to perform the algorithm are present in RSA public class. The additional variables in the class are used for decrypting cipher text using Chinese Remainder Theorem.

4.1.1.7. RSA public Key Encryption Tool Screens

As shown in the Figure 14, the tool has a tab in which the public and private keys are generated. Here the steps required to generate the public and private keys are grouped in such a way that these steps are mapped to the steps in the actual algorithm. By executing these steps the learner can understand the actual algorithm without going through calculating complex arithmetic operations. Learner can generate random prime numbers by clicking the "Generate Primes" button. Random prime numbers are generated as many times the "Generate Primes" button is clicked. Based on the prime numbers, all other values are changed.



Generate Keys

Step 1: Generate two large random primes, p and q

Step 2: Compute n = pq and phi=(p-1)(q-1)

Step 3: Choose e, 1<e<phi, Such tat gcd(e,phi)=1

Step 4: compute the secret exponent d, 1<d<phi, such that ed = 1 (mod phi)

Step 5 : public key is (n,e) private key is (n,d)

Figure 14. Generate keys tab

Figure 15 and Figure 16 shows the encryption and decryption tabs in the RSA public encryption tool.

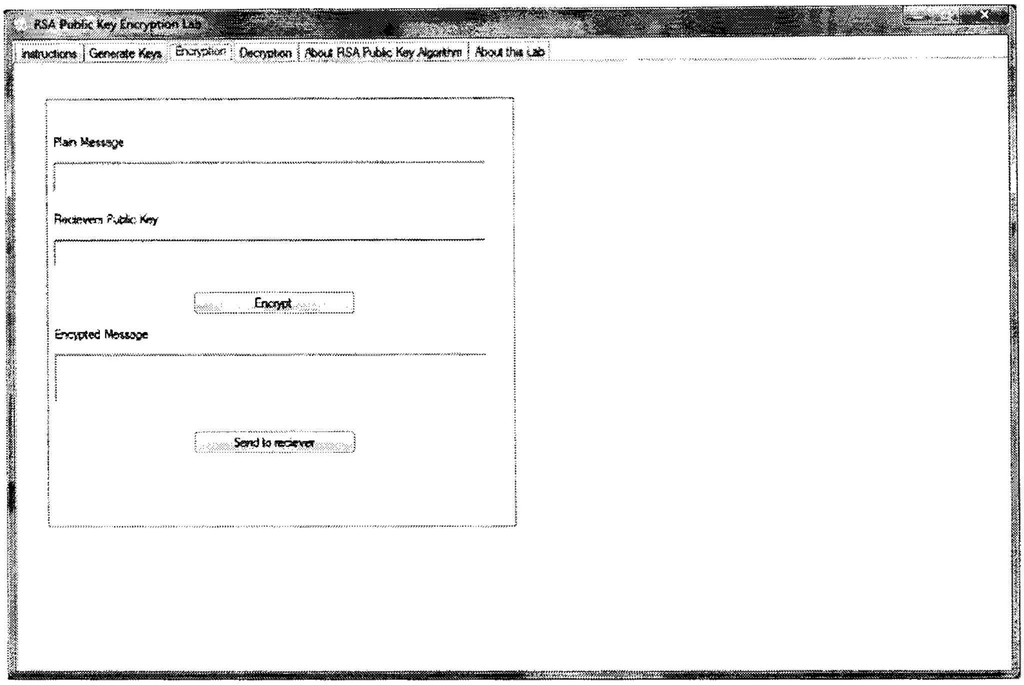


Figure 15. Encrypting

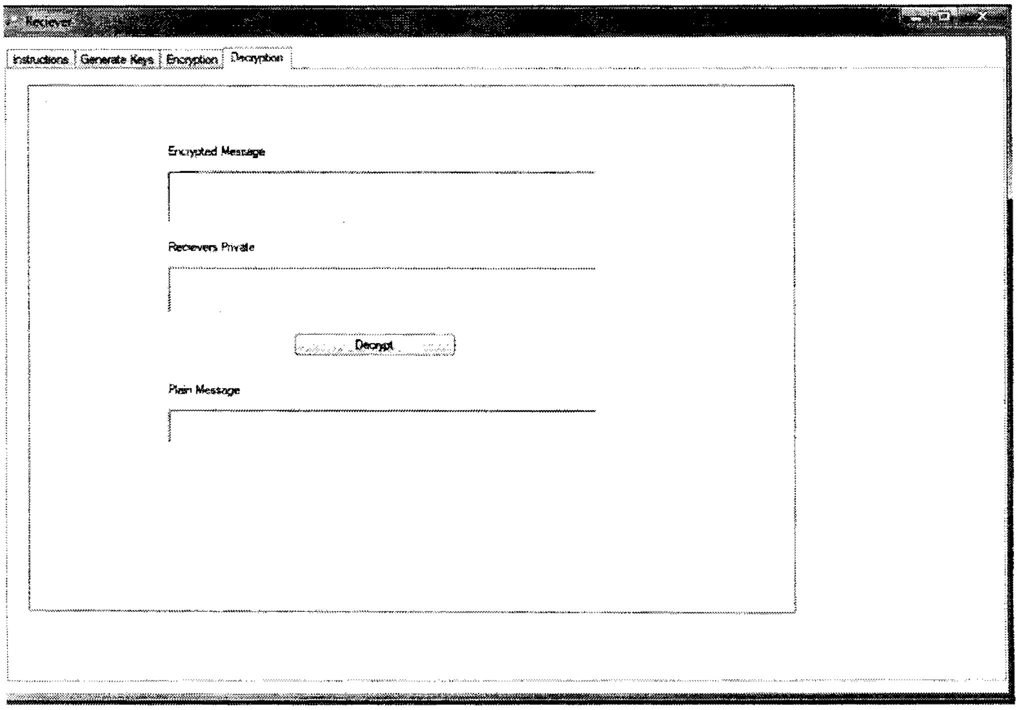


Figure 16. Decrypting

4.2. RSA Public Encryption Tool and the Apply Level

By executing the tool in order to generate the public key, private key and then using those keys in encrypting and decrypting, the learners can learn the actual working model of RSA public key encryption. The tool helps them calculate complex arithmetic calculations. Also, by providing two windows, one for sender and one for recipient, the learner can perform encryption and decryption in both the sender and receiver windows. The steps required to execute the tool are mapped to the steps in the algorithm, so the learners can implicitly recap the understanding of the algorithm in the previous level. This tool will help learners save time calculating when calculating complex arithmetic operations.

4.3. Assessment of the Apply Level

The tool should be executed for assessment in this level. Public keys and private keys should be generated for both the sender and the recipient and encryption and decryption should be performed in both ways. Since this level would reinforce the understanding of the learners, assessment for this level would be difficult. Though there will be no assessment to test the learner attainment in this level, it is important to make sure learners complete the execution of the tool successfully.

5. CONCLUSION, LIMITATIONS AND FUTURE WORK

5.1. Conclusion

Education material and assessments that apply the principles of Bloom's revised taxonomy to help students to learn the concepts of communication security and encryption efficiently were developed. Also, tools like Flash cards which are embedded within the levels of Bloom's taxonomy will help students in the learning activities.

Bloom's revised taxonomy is easy to adapt and can be used as guide in creating the educational material for communication security and encryption. Structured learning, based on levels of difficulties, helps instructors focus on the learners' target understanding level. Selecting the target level of understanding will make learning efficient, and the learners will have a clear understanding of what to accomplish in a particular level and can remain focused, which marks a substantial difference between the learners who are following the structured learning and those who are not. Without structured learning, learners may often try to achieve more than required, which will make learning inefficient.

Bloom's taxonomy is easy to adapt and can be used in designing the course objectives. Increasing or decreasing the targeted levels of attainment is easy when courses are designed with Bloom's taxonomy. Additionally, a course designed with the help of Bloom's taxonomy also helps the learners' learning experience.

Experiential learning is very much suitable for learning cryptographic algorithms. Experiential learning helps learners to retain more when compared to learning through other methods.

Teaching the concepts through graphics wherever possible, instead of teaching through just the text, will help learners gain a better understanding. However, creating or modifying animated material requires more effort.

The combination of the latest technologies like Adobe Flash, Microsoft .NET, Android and tools like Flash cards will be helpful in developing course materials. Mobile phones have become powerful in terms of processing speeds, memory and the network connections, and material content or activities can be designed to deliver over the mobile phone.

The assessment of learners at various levels is important and plays an important role in learning as they drive the way learning is processed. Different types of assessments can test different phases of learning, and having a variety of assessments will keep the learner interested.

5.2 Limitations

The solution presented in this paper has not been tested with the learners. Empirical evidence is lacking to support the suggested use of Bloom's taxonomy in teaching cryptography concepts. The material provided in this paper is a good starting point for understating the concepts but is not comprehensive.

Creating the tools will involve a lot of effort upfront, and major changes to tools using programming languages are not easy. Tools will have the problems of maintainability as any other software artifact is subject to.

Delivering educational content to the mobile phone through applications will be restricted to a particular platform because of incompatibility issues between various platforms. An application developed for an android platform will not be compatible with Apple iphone, Windows 7 phone or any other platforms, and the applications need the same development effort in those platforms.

5.3 Future Work

Adding narration to the animated material makes the accommodation of more learning styles possible. Some learners may prefer voice and learn better if they hear.

Encrypted messages are transmitted over the network from the sender to the recipient. By developing the encryption tool using the typical Client/Server architecture, the encryption and decryption can be done on different computers, which will enable learners to communicate with the encrypted messages and will be more realistic in understanding the encryption concepts.

The RSA public key algorithm is implemented in the advanced languages like C# and Java. These implementations have a variety of options such as specifying the key size up to 2048 bits, specifying secured random number generators, and exporting and importing the keys. Lab exercises can be created using programming languages, which focus on the application of the RSA public key algorithm

This paper can be extended by including the private key encryption algorithm AES. Choosing between the public key and private key algorithms depends on various issues like the size of the content to be encrypted and decrypted, the medium used for the transmission, the security of underlying transmission. Lab exercises can be created by focusing on a selection of these options. Speed can be compared between the public key encryption and private key encryption algorithms.

REFERENCES

1. *.NET Framework Core Development.* http://msdn.microsoft.com/en-us/library/190bkk9s.aspx (accessed August 2010).

2. *.NET Framework Core Development.* http://msdn.microsoft.com/en-us/library/190bkk9s.aspx (accessed August 2010).

3. *Android Flashcards.* http://secretsockssoftware.com/androidflashcards/ (accessed August 2010).

4. *Animation Learning Guide for Flash.* http://www.adobe.com/devnet/flash/learning_guide/animation.html.

5. *Animation Learning Guide for Flash.* http://www.adobe.com/devnet/flash/learning_guide/animation.html.

6. Biggs, John B. "Teaching for quality learning at university." Buckingham: Open University Press/Society for Research into Higher Education, 2003.

7. Bloom, Benjamin S. *Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain.* New York: David McKay Co Inc, 1956.

8. *Bloom's Taxonomy Revised: A Taxonomy for Learning, Teaching, and Assessing.* http://www.transitionmathproject.org/partners/wcp/doc/bloom.pdf (accessed August 2010).

9. Fuller, Ursula and Johnson, Colin G. and Ahoniemi, Tuukka and Cukierman, Diana and Hern\'{a}n-Losada, Isidoro and Jackova, Jana and Lahtinen, Essi and Lewis, Tracy L. and Thompson, Donna McGee and Riedesel, Charles and Thompson, Errol. "Developing a computer science specific learning taxnomy." 152--170. Dundee, Scotland: ACM, 2007.

10. Hazari, Sunil. "Instructional strategies for a graduate level information security management course." In *InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development*, 71-75. Kennesaw, Georgia: ACM, 2004.

11. *Introduction to Android development.* 2010. http://www.ibm.com/developerworks/opensource/library/os-android-devel/.

12. Jumail, D. Rohaya, A. Rambli, and S. Sulaiman. "A design framework for flashcards based guided digital storytelling." *Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on*. Singapore , 2010. 4-8.

13. Lister, Raymond and Leaney, John. "Introductory programming, criterion-referencing, and bloom." *SIGCSE Bull.*, 2003: 143-147.

14. Lorin W. Anderson, David R. Krathwohl, Peter W. Airasian, Kathleen A. Cruikshank, Richard E. Mayer, Paul R. Pintrich, James Raths and Merlin C. Wittrock (Eds.). *A Taxonomy for Learning, Teaching, and Assessing — A Revision of Bloom's Taxonomy of Educational Objectives.* Addison Wesley Longman, Inc, 2001.

15. *A Taxonomy for Learning, Teaching, and Assessing — A Revision of Bloom's Taxonomy of Educational Objectives.* Addison Wesley Longman, Inc, 2001.

16. Mayer, Richard E. "The Promise of Multimedia Learning: Using the Same Instructional Design Methods Across Different Media." *Learning and Instruction* 13, no. 2 (2003): 125-139.

17. Mayer, Richard E. "The Promise of Multimedia Learning: Using the Same Instructional Design Methods Across Different Media." *Learning and Instruction* 13, no. 2 (2003): 125-139.

18. N. Paul, Schembari. "Hands-On Crypto: Experiential Learning in Cryptography." *Proceedng fo the 11th Colloquium for Information Systems Security Education.* 2007. 7-12.

19. Perez-Hardy, Sylvia. "A unique experiential model for teaching network administration." In *CITC4 '03: Proceedings of the 4th conference on Information technology curriculum*, 119--121. Lafayette, Indiana, USA: ACM, 2003.

20. *RSA Algorithm.* http://www.di-mgt.com.au/rsa_alg.html (accessed August 2010).

21. Solms, Johan Van Niekerk and Rossouw Von. "Bloom's Taxonomy for Information Security Education."

22. "Bloom's Taxonomy for Information Security Education."

23. Stefanov, Emil. *C# BigInt: A GNU MP .NET Wrapper - EmilStefanov.net.* 2010. http://www.emilstefanov.net/Projects/GnuMpDotNet/ (accessed August 2010).

24. . *C# BigInt: A GNU MP .NET Wrapper - EmilStefanov.net.* 2010. http://www.emilstefanov.net/Projects/GnuMpDotNet/ (accessed August 2010).

25. *The Developer's Guide | Android Developers.* http://developer.android.com/guide/index.html (accessed August 2010).

26. *The Developer's Guide | Android Developers.* http://developer.android.com/guide/index.html (accessed August 2010).

27. W. Du, K. Jayaram, and N.B. Gaubatz. "Enhancing security education with hands-on laboratory exercises." *5th Annual Symposium on Information Assurance.* Albany, Newyork, 2010. "Enhancing security education with hands-on laboratory exercises." *5th Annual Symposium on Information Assurance.* Albany, Newyork, 2010.

28. *Models --Instructional Design The Taxonomy Table*

http://oregonstate.edu/instruct/coursedev/models/id/taxonomy/#table

APPENDIX

Definitions and Terminology

Message security issues

Confidentiality: The message can be read only by the intended recipient. To all others, the message is unavailable or garbled.

Integrity: It guarantees that the message is not modified during transmission.

Authentication (authorization, verification): Establishes that the sender of the message is actually who they claim to be.

Non-repudiation: Proof that the sender actually sent the message (prevents the author from denying they are the sender)

Attacks and Mechanisms

Security Attack: Any action that compromises the security of information.

Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.

Types of security Attacks

Interruption:

This is an attack on the availability of the system. This happens when an asset is destroyed, becomes unavailable, or cannot be used.

Interception:

This is an attack on confidentiality. Interception occurs when any unauthorized unit gains access to an asset. The unauthorized unit or party could be an individual, a program or even another computer.

Modification:

This is an attack on Integrity. An unauthorized party gains access to a system and make some changes to it: tampering. Examples of such tampering includes the changing of values in a file, altering a program so that it performs differently, and changing the contents of messages that are sent over the network.

Fabrication:

This is an attack on Authenticity. An unauthorized party gains access to the system and inserts false objects into it. Examples of such an attack include a hacker gaining access to a person's email and sending messages. This makes the recipients believe that it is indeed the person sending the message when it is in fact not so, **OR** it could be addition of records to a file.

Cryptography:

The Practice of the enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver

Encryption:

The process of converting plain text into cipher text using a key is called encryption.

Decryption:

The process of converting encrypted cipher text back into plain text using a respective key is called decryption.

Secret Key Encryption:

There will a single key used in this system. Key used for encryption is the same as the one used for decryption.

Public Key Encryption:

There are two keys used in this system: the public key and private key.

The public key: used to encrypt the message. It is widely disseminated, even available in directories like phone books.

The private key: used to decrypt the message. Only the recipient has access to their own private key.

Message authentication:

It is an authenticity verification procedure that facilitates the verification of the integrity of the message as well as the authenticity of the source from which the message is received.

Applications for public key cryptosystems

1. **Encryption/decryption:** The sender encrypts a message with the recipient's public key.
2. **Digital signature:** The sender "signs" a message with its private key.
3. **Key exchange:** Two sides cooperate to exhange a session key.

Examples of Private key Algorithms

- Data Encryption Standard
- Advanced Encryption standard

Examples of Public key Algorithms

- Diffie–Hellman key exchange protocol
- RSA encryption algorithm