Application of Cryptography and Groups

Article · May 2020

CITATIONS
0

READS
2,112

1 author:

Shivakumar Vinod
BITS Pilani, Dubai
1 PUBLICATION **0** CITATIONS

SEE PROFILE

A REPORT

ON

Application of Cryptography and Groups

BY

Shivakumar Vinod Pillai 2018A7PS0245U Computer Science

Prepared in Fulfilment of Project Course CS F266

BITS PILANI, DUBAI CAMPUS
Dubai International Academic City, Dubai UAE

BITS Pilani, Dubai Campus
Dubai International Academic City (DIAC)
Dubai, U.A.E

(January 2020 – May 2020)

A REPORT

ON

Application of Cryptography and Groups

BY

Shivakumar Vinod Pillai 2018A7PS0245U Computer Science

Prepared in Fulfilment of Project Course CS F266

BITS PILANI, DUBAI CAMPUS
Dubai International Academic City, Dubai UAE

BITS Pilani, Dubai Campus
Dubai International Academic City (DIAC)
Dubai, U.A.E

(January 2020 – May 2020)

BITS Pilani, Dubai Campus
Dubai International Academic City (DIAC)
Dubai, U.A.E

Duration: 4 months **Date of Start:** 19-Jan-2020

Title of the Project: Application of Cryptography and Groups

Student Name: Shivakumar Vinod Pillai **Student ID:** 2018A7PS0245U

Discipline of Student: Computer Science Engineering

Name of the Faculty: Dr. Somasundaram Arumugam

Key Words: Groups, Algorithms, Prime Numbers, Cryptography, Key-Exchange, Protocol

Project Areas: Cryptography, Mathematics, Computer Science

Abstract: This report primarily concerns with the study of the applications of cryptography and groups and how each of them are related and can be applied. It also gives an idea on the basics of cryptography along with a study of number theory and its concepts. It focuses on public key cryptosystem, RSA algorithm along with Diffie-Hellman key-exchange protocol and hash functions. It also consists of examples of key-exchange protocols for group based cryptography.

Signature of Student
Date: 9th May 2020

Signature of Faculty
Date:

ACKNOWLEDGEMENTS

Firstly, I would like to express my gratitude to Prof. R. N. Saha, Director BPDC who has given me an opportunity to study in such an esteemed university with all conveniences.

I am also truly grateful to Dr. Somasundaram Arumugam, for giving me the opportunity to work on this project and also for guiding me with all the needed information for the completion of this project and report.

I would also like to Mr. R. Sivakumar, Librarian of BPDC for his help and providing adequate information on the library books and facilities.

CONTENTS

CHAPTER 1: INTRODUCTION

Cryptography is the practice and study of secure communication techniques in the presence of third parties to ensure safe communication. The prefix “crypt” means hidden or “vault” and the suffix “graphy” stands for “writing”.
In this project we primarily focus on the applications of groups and cryptography and how they can be applied.

To begin with this chapter mainly focuses on number theory along with just a brief introduction on cryptography.

Starting off with cryptography, following are the types of cryptographic algorithm which are:

- Secret Key Algorithm

  “The secret key algorithm uses a single key for both encryption and decryption. The set of all secret keys algorithm is known as secret key cryptography, which is sometimes called as conventional cryptography or symmetric cryptography.”

- Public Key Algorithm

  “The basic idea of public key cryptography are public keys. In this each individuals key is separated into two parts, a public key for encryption and a secret key for decryption.”

- Hash Algorithm

  Hash algorithms are based upon a one-way function.
  A function $y = f(x)$ is said to be one- way function, if for every x, it is easy to find y, but for a given y, it is computationally infeasible to get corresponding x.

  “A cryptographic hash function h is a mathematical transformation that takes a message m of any length and convert it into a number of fixed length.”

In cryptography, the number theory and algebra have their role as a basic foundation. Moreover, number theory plays an important role at the centre of interest in application of public key cryptography.

To begin with, following are the basic concepts of number theory:

- Prime Number

  A number when it is only divisible by 1 and itself is a prime number. And when a number is divisible by any other number it is said to be composite.

  Prime numbers have central importance in public key cryptography.

- Greatest Common Divisor

  Consider two integers *m* and *n* then the greatest common divisor of *m* and *n* is the largest integer *d* dividing both *m* and *n* and denoted by *gcd (m,n) = d* or simply *(m,n) = d.*

- Relatively Prime Number

  Two integers *m* and *n* are said to be relatively prime when *gcd(m,n) = 1*

- Modular Arithmetics

  If we divide two integers, *a* by *b* then the relation is, $a = bq + r$

  But in modular arithmetics we use a different approach,

  $$r = a \bmod b$$

  In which *r* is the remainder when *a* is divided by *b,* and we read it as *r* is congruent to *a mod b* or *r* is congruent modulo *b* to *a.*

i) Modular Addition/Subtraction

$$r = (a \pm b) mod\ n = (a\ mod\ n \pm b\ mod\ n)\ mod\ n$$

where *r* is the remainder, when ordinary sum/difference of *a* and *b* id divided by *n*

ii) Modular Multiplication

$$r = ab\ mod\ n$$
$$= (a\ mod\ n \cdot b\ mod\ n)\ mod\ n$$

where *r* is the residue when the ordinary multiplication of *a* and *b* is divided by *n.*

iii) Modular Exponential

$$r = a^b\ mod\ n$$

where r is the remainder when ordinary exponentiation a^b is divided by n.

- Fermat Theorem (Fermat's Little Theorem)

Let *m* be a prime number, then any integer *n* satisfies,

$$n^m \equiv n\ mod\ m$$

And any integer *n* not divisible by *m* satisfies,

$$n^{m-1} \equiv 1\ mod\ m$$

- Euler's Theorem

  i) Euler-Phi Function

  Let *n* be a positive integer, then Euler-Phi function, $\emptyset(n)$ is defined to be the number of positive integers which are less then *n* and prime to *n.*

  Mathematically, i.e., $\emptyset(n)$ = number of elements in the set
  {b: b ≥ 0, b < n and gcd(b,n) = 1}

  ii) $Z_n *$

  Z_n denotes integers from 0 to *n*, Z_n* denotes the set of integers under modulo *n* which is relatively prime to n, for e.g.,

  $$Z_{12}* = \{1, 5, 7, 11\}$$

  Euler Theorem

  It states if *gcd(a,b) = 1,* then $a^{\emptyset(n)} = 1 \, mod \, n$

- Primality Testing

  Primality testing is a criterion for a large number *p* not to be prime. The number maybe prime if it passes primality testing. To be prime, it passes many primality tests and if *p* does not pass any single primality test, then it is sure the *p* is a composite number.

  Very large prime numbers are the backbone of public key cryptography and in many cryptographic algorithms, to select very large prime at random is an essential task.

i) Primality Test based on Fermat Theorem

By Fermat theorem we know that if *p* is a prime number and 0 < a < p then

$$a^{p-1} \equiv 1 \, mod \, p$$

The above congruence holds if *p* is prime.

Pseudoprime: An odd composite number *p* is called a pseudoprime to the base *a* if *gcd(a,p) = 1* and satisfies the Fermat theorem i.e.,

$$a^{p-1} \equiv 1 \, mod \, p$$

ii) Carmichael Number

In the above primality testing, it is possible and can happen that for a composite number *p* such that congruence holds for all possible *a.* In that case, this probability method does not reveal the fact that *p* is composite, and the method fails. In this situation that composite is known as Carmichael number.

"A composite number *p*, which satisfies the congruence $a^{p-1} \equiv 1 \, mod \, p$, for every $a \in Z_p *$ is called Carmichael number."

iii) Solvay-Strassen's Primality Test

If n is a prime number, then it follows that
(1)

$$\frac{a}{n} = a^{\frac{n-1}{2}} \, mod \, n$$

So, if

$$\frac{a}{n} \neq a^{\frac{n-1}{2}} \, mod \, n$$

at that point n is certainly not a prime (i.e., n is a composite number). In any case, there are composite numbers n so that (1) is fulfilled for about a. These numbers are called Euler pseudo-primes with base a. It very well may be understood, that for some random composite number n, there are all things considered n/2 estimations of a not as much as n for which n is a Euler pseudo-prime with base a.

iv) Miller-Rabin Test for Primality

We implement the Miller-Rabin test as follows:

- Given *m*, find *k* so that $m - 1 = 2^k p$ for some odd *p*.
- Pick a random $b \in \{1, \ldots, m-1\}$
- If $b^p = 1$ then *m* passes (and exit).
- For *i = 0, .., k – 1* see if $b^{2^i p} = -1$. If so, *m* passes (and exit).
- Otherwise *m* is composite.

- Finite Field

Finite fields play a key role in that of cryptography, they are the important mathematical tools for cryptographic algorithms.

- Binary Operations

Let G be a non-empty set, binary operation $*$ is a mathematical operator under which

$$\forall\, a, b \in G, a * b \in G$$

- Group

  A non-empty set G with binary operation $*$ is said to be a group if the following properties hold:

  - Associativity: "$\forall\ a, b, c\ \in G; a * (b * c) = (a * b) * c$"

  - Existence of Identity: "$\forall\ a \in G, \exists\ e \in G$ such that $a\ * e = e * a$ the element *e* is called identity element of G with respect to operation $*$."

  - Existence of Inverse: "$\forall\ a \in G, \exists\ e \in G$ such that $a\ * b = e = b * a$. The element *b* is called the inverse of the element *a* with respect to operation $*$."

  Abelian Group:

  "A group G is said to be abelian group with respect to $*$ if $\forall\ a, b, \in G$; $a * b = b * a$. In words, a commutative group is called an abelian group."

- Ring

  A ring denoted by (*R*, +,X) is a non-empty set with two binary operation called addition and multiplication is called ring if the following properties hold:

  - *R* with respect to addition is an abelian group.
  - *R* is associative under multiplication i.e.,
    $$\forall\ a, b, c, \in R; a(bc) = (ab)c$$
  - Distributive laws hold: $\forall\ a, b, c\ \in R$

- Field

  "A commutative ring *R* with multiplicative identity is called a field if every zero element has its multiplicative inverse" mathematically, $\forall a \in R, a \neq 0, \exists b \in R$ such that *ab* = 1

CHAPTER 2: PUBLIC KEY CRYPTOSYSTEM

Whitefield Diffie and Martin Hellman projected a new type of cryptosystem in 1976, known as public key cryptography [PKC], and this invention is one of the most important events in the field of cryptography.

"Public key cryptosystem involves a pair of keys, a public key and a private key associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and a corresponding private key is kept secret."

For instance,
A public key cryptosystem of algorithms representing invertible transformations is a pair of families $\{E_K\}$ and $\{D_K\}$, $K \in$ key space K.

$$E_K : P \rightarrow C \quad and \quad D_K : C \rightarrow P$$

- E_K is the inverse of D_K, for every K.
- It is easy to compute E_K and D_K, for every K.
- For nearly every K, each effortlessly processed calculation equal to D_K is computationally infeasible to get the same from E_K
- Calculating the inverse pairs E_K and D_K from K is feasible for any K.

Ingredients of Public Key Encryption:

- Plain text: "This is readable message or data that is fed into the algorithm as input."
- Encryption Algorithm: "It performs various transformations on the plaintext."
- Public and Private Key: "A pair of keys that have been so as to one is used for encryption and other for decryption."
- Cipher Text: "The scrambled message produced as output and it depend upon plaintext and a key."

- Decryption algorithm: “Algorithm accepts the ciphertext and the matching key and produce original plaintext. As the name suggests the public key of the pair is made public and the private is known to the owners.”

Advantages and Disadvantages of Public Key Cryptography

- The primary benefit of public key cryptography is improved convenience and security *i.e.,* private keys need not be communicated to anyone. While in the secret key system the secret key should be communicated.
- The other major benefit is that they can provide technique for digital signature. The verification via secret key systems require the distribution of some secret and occasionally require confidence of a third party as well.
- A drawback of using public key cryptography for encryption is its swiftness, and in secret key encryption there are some methods that are faster than public key encryption.
- Public key cryptography is theoretically useful for impersonation. However, even if the user does not have a private key. A effective attack on the certification authority would allow an opponent to impersonate whoever even the opponent prefers to attach a key of the opponent's choice to another user's name by using a public key certificate from the compromised authority.

- RSA Cryptosystem:

In 1977, Ronald Rivest, Adi Shamir, and Leonard Adleman were to make the single most spectacular contribution to the public key cryptography: took up the challenge of producing of producing a full-fledged public key cryptography: RSA Cryptosystem.

The RSA cryptosystem is based on the factorization complexity of two great primes. In this cryptography, we assume there is a key centre. The key centre:

- Chooses two extremely large primes e and r
- Calculates $n = e.r$ and $\emptyset(n) = (e-1)\,.\,(r-1)$
- For every user, chooses randomly integer p; $1 \leq p \leq \emptyset(n)$ and $\big(p, \emptyset(n)\big) = 1$
- For every user, computes d, the multiplicative inverse of $p.mod\ \emptyset(n)$ by Euclidean algorithm.

- Security of RSA:

Three potential ways to deal with assaulting the RSA algorithm:

1. Brute force: That trying all possible private keys. “The success/failure of the brute force attack depends upon the length of key space used by the respective cryptosystem.” By using large key space, it is possible to avoid the brute force attack. RSA cryptosystem use the key space as large as possible for the performance and to avid this attack.
2. Mathematical attack: “Several approaches equivalent in effect to factoring the product of two primes.”
3. Timing attacks: “These depend on the running time of decryption algorithm.”

RSA Problem: “In cryptography the problem is the task of finding e^{th} roots modulo a composite number N whose factor are not known.”

Full decryption of an RSA ciphertext is assumed to be unfeasible on the basis that both of these problems are difficult. There is no efficient algorithm to solve them. Providing protection against partial decryption will require a safe padding scheme to be added.

- Key Management:

Public key cryptography makes key management easier. The public key cryptography has two aspects to utilize.

1. The circulation of public key.
2. The usage of public key for sharing hidden encryption keys.

- Diffie Hellman’s Key Exchange System

“Diffie-Hellman was the first public key algorithm that allows two parties that have no prior knowledge of each other to establish a shared secret key over an insecure communication channel.”

The system works as follows:

- The user A chooses a secret integer $a < p$ and computes
$$\alpha = g^a \bmod p$$
He/she sends α to the user B.
- The user B chooses a secret integer $b < p$ and computes
$$\beta = g^b \bmod p$$
He/she sends β to the user A.
- The user A computes $k = \beta^a \bmod p$
- The user B computes $k = \alpha^b \bmod p$

In this way both users agree upon a common secret key, k.

Diffie Hellman key exchange system is based on the difficulty of discrete logarithm.
Discrete Logarithm Problem says that, "let X be a cyclic group and x a generator of X. Given $h \in X$, find an integer t such that $x^t = h$."

"In particular Diffie Hellman key exchange uses finite cyclic groups."

- ElGamal Cryptosystem

The ElGamal scheme is a variant of the Diffie Hellman scheme which incorporates an enciphering algorithm. The ElGamal Scheme is primarily designed for signing purposes, as opposed to RSA, which can be used as both a public key cryptosystem and signature scheme.

ElGamal encryption consist of three components:

- Key Generation
  1. X choose a random x from {0, …., $q-1$}
  2. X computes $j = g^x$
  3. X publishes j along with q and g as public key.
  4. $'x'$ is the private key which must keep secret.
- Encryption Algorithm
  To encrypt message m to A under public key (q, g, j)
  1. Y choose a randomly y from {0, …, $q-1$} and calculate
  $$c_1 = g^y$$
  $$c_2 = m \,.\, j^y$$
  2. Y sends the ciphertext to X.
- Decryption Algorithm
  To decrypt ciphertext (c_1, c_2) by private key x.
  1. X compute $\frac{c_2}{c_1^x}$ as plaintext message.
  2. The decryption algorithm produces the intended message
  $$\frac{c_2}{c_1^x} = \frac{m \,.\, j^y}{g^{xy}} = \frac{m \,.\, g^{xy}}{g^{xy}} = m$$

- Hash Function

"Hash function are based upon a one-way function. A function $y = f(x)$ is said one-way function if for every x, it is easy to find y, but for a given y, it is computationally infeasible to get corresponding x."

Hash function should satisfy the following the following two properties:

- It must be cryptographically secure/computationally infeasible. We can say that it is not possible. To find a message that has given pre specified hash value message digest. This property is called one-way property.
- It should be impossible to find any two messages that have the same hash value.

  - Application of Hash Function to Public Key Cryptography

A check sum is the outcome from computational algorithm following up on the data being referred to such an extent, that if a solitary piece of that data changes, the subsequent check as a whole will change, and the generation of such check sum with an assortment of computational algorithm known as one-way hash functions. Through these functions, we can process an enormous assortment of data and determine a lot smaller arrangement of guidelines alluded to as hash code.
Hash function is used to solve this problem, no third party can check the validity and authenticity of the message. To solve this problem, digital signature is an important cryptographic tool provided by public key cryptography. Generation of digital signature is based on hash function.

CHAPTER 3: GROUP BASED CRYPTOGRAPHY

There are numerous group-based cryptographic protocols, and most of the cryptographic schemes still use groups. Diffie Hellman key exchange, for example, makes use of finite cyclic groups.

“In non-commutative cryptography which is a field of cryptography in which the cryptographic primitives, methods and systems are based on groups, semigroups and rings, and these protocols are developed for solving cryptographic problems like key exchange, encryption, decryption and authentication.”
In comparison, the commonly used public key cryptosystems such as the RSA cryptosystem, Diffie Hellman key exchange, and elliptical curve cryptography are based on number theory and, consequently, on algebraic commutative structures.

Following are the examples of group-based cryptography:

- Shpilrain-Zapata public-key protocol

Utilizing this protocol, we can structure a cryptosystem with the following highlights:

1. Bob transmits an encrypted binary sequence that is correctly decrypted by Alice with very high probability of 1.
2. Eve, the opponent given arbitrarily high computational speed, cannot clearly identify the bits in Bob's binary series, using a brute force attack.

Despite computational speed given to Eve there is no guarantee that her brute force attack will produce decisive results.

- Magyarik-Wagner public key protocol

Utilizing this protocol, we can structure a cryptosystem with the following highlights:

X is a finite generator set, and let P and Q be finite relator sets on X. Consider the two groups G, G_0 with presentations

$$G = (X; P) \quad and \quad G_0 = (X; P \cup Q)$$

In this protocol the public key is $(X; P)$ and the words w_0 and w_1

And for encrypting a single bit, $i \in \{0,1\}$, pick w_i and it is transformed it into a ciphertext word w by randomly and repeatedly applying the transformations (T1) and (T2) for the presentation (W, P).

And for decrypting a word w, we run the algorithm for the word problem of G' in order to decide ww_0^{-1} and ww_1^{-1} is equivalent to the empty word for the presentation $(X; P \cup Q)$

And the private key is the set Q.

- Anshel-Anshel-Goldfeld key exchange

Utilizing this protocol, we can structure a cryptosystem with the following highlights:
Let X be a fixed nonabelian group

- Public information:
  - Alice's public key is a tuple of elements, $a = (a_1, \dots, a_n)$ in X
  - Bob's public key is a tuple of elements $b = (b_1, \dots, b_n)$ in X

- Private Information:

    - Alice's private key is a sequence of elements from a and their inverses: $a_{i_1}^{\varepsilon_1}, \dots, a_{i_L}^{\varepsilon_L}$, where $a_{i_k} \in a$ and $\varepsilon_k = \pm 1$. Based on that sequence she computes the product $A = a_{i_1}^{\varepsilon_1}, \dots, a_{i_L}^{\varepsilon_L}$
    - Bob's private key is a sequence of elements from b and their inverses: $b_{j_1}^{\delta_1}, \dots, b_{j_L}^{\delta_L}$, where $b_{j_k} \in b$ and $\delta_k = \pm 1$. Based on that sequence she computes the product $B = b_{j_1}^{\delta_1}, \dots, b_{j_L}^{\delta_L}$

- Transition:

    - Alice sends a tuple $\bar{a} = (A^{-1}\, b_1 A, \dots, A^{-1}\, b_n A)$ to Bob.
    - Bob sends a tuple $\bar{b} = (B^{-1}\, a_1 B, \dots, B^{-1}\, a_n B)$ to Alice.

- Shared Key:

    The shared key by Alice and Bob is the group element $K = A^{-1}B^{-1}AB \in G$ called the commutator of $A\ and\ B$.

    - Alice computes K as a product $A^{-1} \cdot \left(B^{-1}\, a_{i_1}^{\varepsilon_1} B\right) \dots \left(B^{-1}\, a_{i_L}^{\varepsilon_L} B\right) = A^{-1}\, B^{-1}\, AB$.
    - Bob computes K as a product $\left(A^{-1}\, b_{i_1}^{\varepsilon_1} A\right) \dots \left(A^{-1}\, b_{i_L}^{\varepsilon_L} A\right) \cdot B$

- Ko-Lee Key Exchange Protocol

Utilizing this protocol, we can structure a cryptosystem with the following highlights:

- Alice and Bob agree publicly agree on a non-abelian group X with an abelian subgroup C.
- They publicly agree on $w \in X$.
- Alice then secretly sends $a \in C$ and sends w^a to Bob.
- Bob then secretly sends $b \in C$ and sends w^b to Alice.
- Alice then computes $K_a = (w^b)^a = w^{ba}$
- Bob then computes $K_b = (w^a)^b = w^{ab}$
- The resultant private key is $K = K_A = K_B$ as $a, b \in C$

- Stickel's key exchange protocol

Utilizing this protocol, we can structure a cryptosystem with the following highlights:

- "Let X be a public non-abelian finite group.
- Let a, b be public elements of X such that $ab \neq ba$. Let the orders of $a \; and \; b$ be $N \; and \; M$ respectively.
- Alice picks two random numbers $n < N \; and \; m < M$ and sends $u = \; a^m \; b^n$ to Bob.
- Bob chooses two random numbers $r < N \; and \; s < M$ and sends $v = \; a^m b^n$ to Alice.
- The common key shared by Alice and Bob is $K = \; a^{m+r} b^{n+s}$
- Alice computes the key by $K = \; a^m v b^n$
- Bob computes the key by $K = \; a^r u b^s$"

- Conjugacy Search Problem

"Let X be a non-abelian group, and let $g, h \; \in X$ be such that $h = \; g^x$ for some $x \; \in X$. For the given elements $g \; and \; h$, find an element $y \; \in X$ such that $h = \; g^y$"

Let us suppose that we find a group where the conjugacy search problem is hard, it is possible for one to define cryptosystems that are similar to cryptosystems based on discrete logarithmic problem. As discussed above Ko et Al had proposed an analogue of Diffie-Hellman Key agreement protocol.

- Symmetric Schemes

Group theory is being used in proposals of public key cryptosystems and key exchange schemes, along with symmetric cryptography. Hash function is an area of symmetric cryptography where the concepts of groups have been used and hash function are a vital component of many cryptographic protocols. One of the most used example of hash functions is SHA-1, where SHA stands for Secure Hash Algorithm.

CONCLUSION

This project was done to study about to the applications of cryptography and group, and I came up with the following conclusions after going through text books and research papers. Group-based cryptography is yet in development and an efficient cryptosystem is yet to emerge despite the protocols being put forward by Ko et al. and Anshel et al. being good ideas. Great care has to be taken with the choice of group as those with lower degrees are at a greater risk to attacks. There has been significant advances in the field of infinite groups but on the other hand, finite groups still require more discoveries and it would in turn be better as it is more advantageous than infinite group cryptography.

REFERENCES

[1] Dr. Manoj Kumar, Cryptography and Network Security, Fourth Edition (2013)

[2] Sunil Gupta, Introduction to Cryptography and Network Security, Second Edition (2013)

[3] Chey Cobb, Cryptography for Dummies, 2004

[4] Simon R. Blackburn, Carlos CID and Ciaran Mullan, Group Theory in Cryptography, 2010

[5] Priya Arora, Use of Group Theory in Cryptography, 2016

[6] Vladimir Shpilrain and Alexander Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient, 2004

[7] Vladmir Shpilrain and Gabriel Zapata, Using decision problems in public key cryptography, 2007

[8] Jean-Camille Birget, Spyros Magliveras and Michal Sramka, On public-key cryptosystems based on combinational group theory, 2005

[9] Christopher Lloyd, The Ko-Lee exchange protocol with generalized dihedral groups, 2016

[10] Tom St Denis, One-way hash function, Cryptography for developers 2007

[11] Ben Lynn, Cryptography notes, Stanford University