# Cryptography & Encryption:6G7Z1011

Keith Yates

February 8, 2019

# Cryptography & Encryption:6G7Z1011 : Mathematical Structures and a First Look at Diffie

Keith Yates

February 8, 2019

# Overview

We continue with our study of real world (that is algorithms currently used in secure systems) cryptography. Goals of the lecture:

1. To define, discuss and work with the key mathematical structures used in Cryptography
2. Discuss the Diffie-Hellman key exchange protocol; this result started Public Key Cryptography [1] .

# Groups, Rings and Fields

We have meet $\mathbb{Z}(n)$ under addition and multiplication, and we have used it in a few cases; it was just 'clock' arithmetic. A fact glossed over till know is the role of $n$. We have already seen that $\mathbb{Z}(6)$ and $\mathbb{Z}(7)$ are very different structures:

1. In $\mathbb{Z}(6)$ two non-zero elements could multiply to zero; for example, $2 \times 3 = 0$
2. In $\mathbb{Z}(7)$ two non-zero elements never multiplied to zero.

There are three fundamental algebraic constructs that we need to define.

# Definition:Group

A *group* $G$ is a set with an operation $\circ : G \times G \to G$; for brevity we write $g_1 g_2$ for $g_1 \circ g_2$. The operation satisfies:

1. The operation is associative that is $(g_1 g_2) g_3 = g_1 (g_2 g_3)$.
2. There is an identity (which we denote by 1 ) such that $1g = g1$ for all $g \in G$.
3. To every $g \in G$ there is an inverse $g^{-1}$ such that $gg^{-1} = 1$.

If $g_1 g_2 = g_2 g_1$ holds for all $g_1$, $g_2 \in G$ then we have an *abelian group*.

# Ring

A *ring* $R$ is a set with two operations $+ : G \times G \to G$ (addition) and $\times : G \times G \to G$ multiplication.

1. $(G, +)$ is an abelian group
2. Multiplication is associative; $(a \times b) \times c = a \times (b \times c)$.
3. Multiplication is distributive; that is

$$a(b + c) = ab + ac \quad \text{and} \quad (b + c)a = ba + ca. \quad (0.1)$$

# Field

A *field* $F$ is a commutative ring in which every non-zero element has a multiplicative inverse.
The definitions of group, ring and field are abstract; we illustrate the definitions with some examples and classify them.

# Examples

Groups are an abstract concept the 1 in a group is the identity element it means $1g = g$ for all $g$ (it does not have to be the number 1) Decide if the following are groups and if they are determine if they are abelian, you need to decide what the identity is, and if each element has an inverse.

1. $\{1, 2, 3, \ldots\}$ under addition.
2. $\{\ldots, -2, -1, , 0, 1, 2, 3, \ldots\}$ under addition.
3. All two by two matrices under addition.
4. All two by two matrices under multiplication.
5. The set of bijections on a set $X$ under function composition.

# $S_3$

The collection of bijective functions on three elements (under function composition) is a non-abelian group. It is denoted by $S_3$ and its termed the *permutation group* on three objects (permutation groups are used a lot in cryptography)

1. What size is the group?
2. Can we evaluate its multiplication table?

This will get messy, in lectures we will experiment with small groups, in labs slightly larger groups.

# $S_3$

Even with small groups, we need to use a simplified notation, this is going to get messy. First recall a bijection is an injective and surjective function.

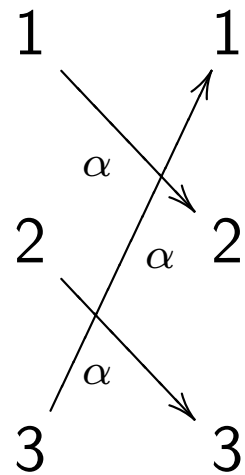


Table: A bijection between three objects. It is to be read: the bijection $\alpha$ takes 1 to 2, 2 to 3 and 3 to 1

# Composition of bijections

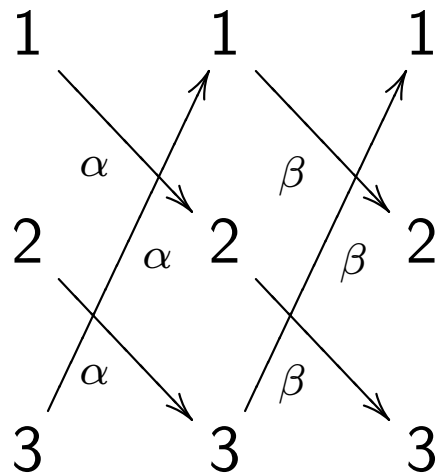


Table: The compostion of two bijections is a bijection; $\beta\alpha$, so for example $\beta\alpha(1) = 3$

# Shorthand

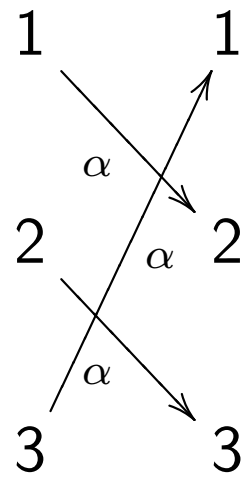


Table: $\alpha = (1, 2, 3)$

The bijection $\alpha$ may be written $(1, 2, 3)$ and it reads $1 \mapsto 2$, $2 \mapsto 3$ and $3 \mapsto 1$.

# Evaluate $S_3$

It will be a bit messy, but construct the multiplication table for $S_3$ To help you let us agree to write

1. $e$ for the bijection that fixes 1, 2 and 3, so does nothing!
2. $a = (1, 2, 3)$
3. $b = (2, 3)$

# What does $S_3$ look like?

Blanks you need to fill in

| . | $e$ | $a$ | $a^2$ | $b$ | $ab$ | $a^2b$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $b$ | $ab$ | $a^2b$ |
| $a$ | $a$ | | | | | |
| $a^2$ | $a^2$ | | | | | |
| $b$ | $b$ | | | | | |
| $ab$ | $ab$ | | | | | |
| $a^2b$ | $a^2b$ | | | | | |

Table: $S_3$

# Distinguishing between Groups

We have shown $S_3$ is a groups and its size is 6. The next question is

1. Are there any other groups of size 6 that are different from $S_3$?
2. If so, what do they look like?

# Homomorphism, Isomorphism

We need to define what we mean by two groups being the same, and to turn it around what it means for two groups to be different. It is, hopefully, obvious that for two groups to be identical they need to have the same size. A *isomorphism* is a bijection between two groups

$$\phi : G_1 \to G_2, \quad g_1 \mapsto \phi(g_1) \tag{0.2}$$

such that

$$\phi(a \circ_{G_1} b) = \phi(a) \circ_{G_2} \phi(b) \tag{0.3}$$

holds for all $a$, $b \in G$.

# Isomorphism

Let us find a simple example of two groups of the same size but they are not isomorphic.

1. $S_3$
2. $\mathbb{Z}(7)^*$

The important point:

1. For a given integer $n$ there may exist numerous distinct groups of that size.

# Symmetric and Asymmetric

Recall

1. A key is termed *symmetric* if the key both encrypts and decrypts a message. For example, the one time pad with any key 010001001101 . . . is symmetric, if you apply it twice you end up back where you started.
2. A key is termed *asymmetric* if the key that encrypts a mess-sage is different form the key that decrypts it; for example the Caesar cipher is asymmetric because the encryption and decryption keys differ.

# Public /Private

We first need to clarify the difference between Public and Private cryptography. All examples prior to today's lecture are examples of private key cryptography. That is Alice and Bob have a private key by which they can securely communicate; for example Alice and Bob could use the one time pad with a particular key

$$K = 0100101010101010 \tag{0.4}$$

The key needs to be kept private, if Eve knows the value of the key then they can decrypt the message.

# Some Notation

Our protagonists are still, Alice, Bob and Eve. The goal remains the same: Alice and Bob wish to communicate securely and Eve wishes to pry. We introduce

$$K_{A,Pu} = \text{Alice's Public Key known to All} \tag{0.5}$$

and

$$K_{A,Pr} = \text{Alice's Private Key known only to Alice} \tag{0.6}$$

$K_{B,Pu}$, $K_{B,Pr}$, $K_{E,Pu}$ and $K_{E,Pr}$ all have the obvious meanings.

# Secure Connection across an Insecure Channel

The following is very important (and concepts such as e-commerce depend critically upon it)

## Secure connection

The Diffie-Hellman algorithm allows Alice and Bob to establish a secure connection across an insecure connection.

If the above statement does not surprise you - you should think about it a little more

# Alice, Bob and Eve in a Cafe

Forget about computers and the internet; imagine Alice, Bob and Eve meet in a cafe they have never meet and have no knowledge about each other. Alice and Bob wish to establish a 'shared secret' (typically this is a number) Given Eve is sat with them and Eve hears every word they say to each other how is it possible for Alice and Bob to exchange information and generate a 'shared secret'.
Note : Alice and Bob have never meet.

## How it this Possible?

It was for many years thought to be impossible to establish a secure connection over an insecure network. The solution involves complicated ideas from discrete mathematics.

# e-commerce variant

The e-commerce variant of the previous problems occurs frequently. Whilst in some e-commerce sites (Amazon) you have an account there are many sites you use for one off transactions in which your computer and the website of the company you are buying from establish a secure connection over an insecure channel
We commence the non-trivial task of showing how to do this.

# Diffie Protocol

Fix a large prime $p$ and a integer $g \mod p$; these numbers are known to Alice, Bob and Eve (in fact anyone in the world) can know their values. The protocol is as follows:

1. Alice picks a secret integer $a$.
2. Bob picks a secret integer $b$.
3. Alice works out $A = g^a \mod p$ and Bob works out $B = g^b \mod A$.
4. Alice sends $A$ to Bob, Bob sends $B$ to Alice; note Eve has knowledge of $A$ and $B$. (Everybody knows the values of $A$ and $B$.)
5. The clever bit follows;
   a) Alice computes $A' = B^a \mod p$
   b) Bob computes $B' = A^b \mod p$.

# Congruent Mathematics

We find

$$A' = B^a = (g^b)^a = (g^a)^b = A^b = B' \mod p. \qquad (0.7)$$

Alice and Bob determine the same number and this is their 'shared secret'
We need an example with real numbers

# Lab Question

We work on the Java Implementation of the Diffie-Hellman protocol. We will use small prime numbers — if a question asks you to verify something you are free to use a brute force attack.

1. Let $p = 941$ (prove 941 is prime), we let $g = 237$.
2. Suppose Alice chooses a secret key $a = 347$ what is $A$?
3. Suppose Bob chooses a secret key $b = 781$ what is $B$?
4. What is the value of $A'$?
5. What is the value of $B'$?

# Knowledge is Power

At this point we have shown how Alice and Bob can generate a shared key — why is Eve not in a position to find $A'$.

| | $p$ | $g$ | $a$ | $b$ | $A$ | $B$ |
|---|---|---|---|---|---|---|
| Alice | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Bob | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ |
| Eve | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |

Table: Who knows what, a ✓indicates the person knows the value of the variable. Alice and Bob are one piece of data short, Eve — crucially is two pieces short — recall the goal is to evaluate $A'$ (or $B'$ as $A' = B'$).

# Eve's hard problem

We left Eve trying to work out Alice and Bob's shared secret. Recall this amounts to solving

$$627^a = 390 \mod 941 \quad \text{or equivalently} \quad 627^b = 691 \mod 941. \tag{0.8}$$

A lab question asks you to 'crack' the problem by brute force; in our toy model $p = 941$ so brute force will work.

## What are real world values?

Our algorithm is a correct implementation of Hiffie, however in real world encryption our primes are of the size $2^{1000}$.

# Diffie-Hellman Problem

If Eve discovers an algorithm that can solve the equations

$$x^a = y \mod p \quad \text{or equivalently} \quad x^b = c \mod p. \tag{0.9}$$

in a reasonable amount of time then the Diffie algorithm would be obsolete.
No one has yet found such an algorithm, and the study of eqn. 0.9 is referred to as the 'Diffie-Hellman' problem.

# The Diffie-Hellman Problem

The Diffie-Hellman problem can be cast into a precise mathematical statememt; to do this we need to introduce some new mathematical concepts.
(There is little I can do about this as cryptography becomes more advanced computer scientists use ideas from more abstract areas of mathematics, for example elliptic curves.)

 W. Diffie and M.E.Hellman, *New directions in cryptography*, IEEE Trans. Information Theory, (1976).