Cryptography & Encryption:6G7Z1011

Keith Yates

February 15, 2019

Cryptography & Encryption:6G7Z1011 : Coding Diffie

Keith Yates

February 15, 2019

Overview

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

1. Discuss the Diffie-Hellman key exchange protocol; this result started Public Key Cryptography [1] .
2. Implement Diffie-Hellman in JAVA
3. Assess the security of Diffie-Hellman

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

$$K = 0100101010101010 \tag{0.1}$$

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

$$K_{A,Pu} = \text{Alice's Public Key known to All} \tag{0.2}$$

and

$$K_{A,Pr} = \text{Alice's Private Key known only to Alice} \tag{0.3}$$

$K_{B,Pu}$, $K_{B,Pr}$, $K_{E,Pu}$ 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 $B = g^b \mod p$.
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

$$A' = B^a = (g^b)^a = (g^a)^b = A^b = B' \mod p. \tag{0.4}$$

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

$$627^a = 390 \mod 941 \quad \text{or equivalently} \quad 627^b = 691 \mod 941. \tag{0.5}$$

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

$$x^a = y \mod p \quad \text{or equivalently} \quad x^b = c \mod p. \tag{0.6}$$

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. 0.6 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.)

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*.

Example

Let us write $\mathbb{Z}(7)^* = \mathbb{Z}(7) \setminus \{0\}$; that is we remove the zero element (this is common notation). Evaluate the multiplication tables for

$$(\mathbb{Z}(7)^*, \times) \quad \text{and} \quad (\mathbb{Z}(6)^*, \times). \tag{0.7}$$

In our new terminology one of the above sets is an abelian group — which one is it?

Examples

Groups are an abstract concept the 1 in a group is the identity element it means $1g = g$ for all g. Decide if the following are groups and if they are abelian.

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 used in encryption

Recall S_3 is the group of permutations on three objects, we illustrate its usage in a 'toy encryption model', S_3 will be used to permute the blocks and the data in the blocks. It is a useful first approximation to the DES. Define a key

$$K = (\alpha, \beta, \alpha, \beta). \tag{0.8}$$

$\alpha = (1, 2)$, $\beta = (1, 2, 3)$. We define an encryption action on a string of length 9 by letting β act on the 3 blocks, and then applying α on the first block, β on the second block and α on the third block. Consider the string abcdefghi

$$\mid \mathrm{a} \mid \mathrm{b} \mid \mathrm{c} \mid \mathrm{d} \mid \mathrm{e} \mid \mathrm{f} \mid \mathrm{g} \mid \mathrm{h} \mid \mathrm{i} \mid$$

$$\mid \mathrm{a} \mid \mathrm{b} \mid \mathrm{c} \,\|\, \mathrm{d} \mid \mathrm{e} \mid \mathrm{f} \,\|\, \mathrm{g} \mid \mathrm{h} \mid \mathrm{i} \mid$$

We need to draw diagrams.

More Theory

To make headway we need to develop some more theory, some new concepts:

1. Equivalence relation;
2. Subgroup;
3. Generators;
4. Coset.

Relation, Equivalence Relation

Let X denote a set a *relation* R is simply a subset of $X \times X$. As *equivalence* relation is a relation that is

1. reflexive: that is, $(x, x) \in R$ for all $x \in X$
2. symmetric: that is, $(x, y) \in R$ implies $(y, x) \in R$
3. transitive: that is, $(x, y) \in R$ and $(y, z) \in R$ imply $(x, z) \in R$

We write $x \sim y$ if $(x, y) \in R$

Examples

We need some examples:

1. In $\mathbb{Z}$ (set of all integers) define $x \sim y$ if and only if $x - y$ is a multiple of 10.
2. In $\mathbb{Z}$ (set of all integers) define $x \sim y$ if and only if $x \leq y$

Prove $\sim$ is an equivalence relation in 1, but $\sim$ is not an equivalence relation in 2.

Equivalence relations partition a set X

Let X denote a set, and $\sim$ an equivalence relation. For each $x \in X$ define

$$x^{\bullet} = \{y \in X \mid x \sim y\} \tag{0.9}$$

An equivalence relation partitions the set X. That is

$$X = \sqcup_{i=1}^{n} x_i^{\bullet} \tag{0.10}$$

where $\sqcup$ is disjoint union. A picture may help

Partitions

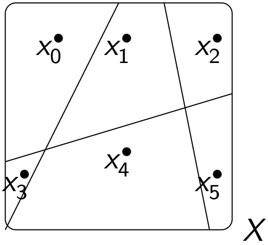

Figure: An equivalence relation partitions a set X into disjoint components.

Equivalence Relations

⌜An equivalence $\sim$ relation on a set X partitions a set; that is

$$X = \sqcup_{i=1}^{n} x_i^\bullet \tag{0.11}$$

⌟

Proof.

Let x, $y \in X$ then we claim either $x^\bullet = y^\bullet$ or $x^\bullet \cap y^\bullet = \emptyset$.
Have a go!

□

proof

Proof.

Recall

$$x^\bullet = \{a \in X \mid x \sim a\} \quad \text{and} \quad y^\bullet = \{a \in X \mid y \sim a\}\,. \tag{0.12}$$

and suppose $x^\bullet \cap y^\bullet \neq \emptyset$. There is a $z \in X$

$$z \in x^\bullet \cap y^\bullet. \tag{0.13}$$

we have $x \sim z$ and $y \sim z$.

1. Pick any $\alpha \in x^\bullet$, then $x \sim \alpha$ so $\alpha \sim x$ (symmetric) and as $x \sim z$ then $\alpha \sim z$ and as $z \sim y$ then $\alpha \sim y$ so $\alpha \in y^\bullet$. We deduce $x^\bullet \subseteq y^\bullet$.
2. Similarly $y^\bullet \subseteq x^\bullet$

□

Subgroup

Let G denote a group, a subset of G is termed a subgroup if it is itself a group. For example

$$GL(2) = \left\{L \in M_{2,2}(\mathbb{R}) \mid L^{-1} \text{ exists}\right\} \tag{0.14}$$

(recall $M_{2,2}(\mathbb{R})$ is the set of 2×2 matrices) is a group and

$$H = \left\{\begin{pmatrix} a & c \\ 0 & d \end{pmatrix} \mid ad \neq 0\right\} \tag{0.15}$$

is a subgroup of $GL(2)$

Prove H is a subgroup

1. Is H closed under multiplication?
2. Does H has an identity?
3. Does each element have an inverse?
4. Is multiplication associative?

Prove H is a subgroup

1. Is H closed under multiplication? Yes
2. Does H has an identity? Yes
3. Does each element have an inverse? Yes

$$A = \begin{pmatrix} a & c \\ 0 & d \end{pmatrix} \quad \text{then} \quad A^{-1} = \frac{1}{ad}\begin{pmatrix} d & -c \\ 0 & a \end{pmatrix} \tag{0.16}$$

Generator

Let g be an element of a group G then we write

$$\langle g \rangle \tag{0.17}$$

for the smallest subgroup in G that contains g, and if A is a subset of G then we write

$$\langle A \rangle \tag{0.18}$$

for the smallest subgroup of G that contains A.

Examples

Let us return to our favourite group S_3

$$a = (1, 2, 3) \quad \text{and} \quad b = (2, 3) \tag{0.19}$$

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

What are $\langle a \rangle$ and $\langle b \rangle$?

Subgroup

Easy

$$\langle a\rangle = \left\{a, a^2, a^3\right\} = \left\{a, a^2, e\right\} \tag{0.20}$$

and

$$\langle b\rangle = \left\{b, b^2\right\} = \{b, e\}\,. \tag{0.21}$$

Coset

Let H be a subgroup of G then the *right coset* of H by $g \in G$ is the set

$$Hg = \{hg \mid h \in H\} \tag{0.22}$$

The Cosets of S_3 by $\langle a \rangle$

Work out the cosets of S_3 by $\langle a \rangle$.

order

The number of elements in a group is termed its order and is denoted $|G|$, For example:

1. $|S_3| = 6$
2. $|\langle a \rangle| = 3$
3. $|\langle b \rangle| = 2$

Assess Security of Diffie-Helman

Read up on this, I will cover it later

CW1

Your assignment is out.

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