# **Normal Logarithms**

Graphical user interface, application

Description automatically generated

To compute the exponent from answer is not an easy task.

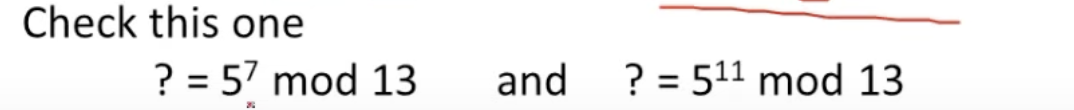
# **Modular Arithmetic**

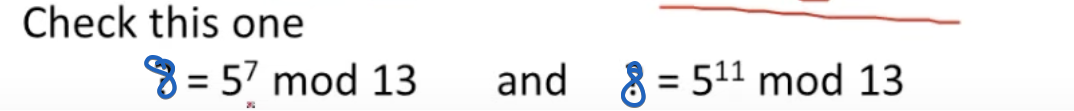
Graphical user interface

Description automatically generated with medium confidence

Text

Description automatically generated





We are getting the same result for different values of i.  
Is i = 3,7 or 11 for 5^i mod 13 ??

Discrete logarithms should produce unique resultsA picture containing text

Description automatically generated

# **Primitive Roots**

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated with medium confidence

For unique value of i 🡪 b should be the primitive root of the prime modulo m.

Calendar

Description automatically generated with medium confidence

For m=13, if I select b= 2,6,7,11   
then only we will get unique values for i.

Text

Description automatically generated with medium confidence

Using Brute Force approach and finding i for large numbers is very difficult.  
So this primitive roots concept of finding i 🡪 tough for large mod value.  
 🡪 easy for small mod value.

# **Purpose of Diffie Hellman Key Exchange Algorithm**

Text

Description automatically generated

In Symmetric cryptography key must be shared first, then only decryption takes place at the receiver side.

Text

Description automatically generated

Logo

Description automatically generated with medium confidence

Agent-X and Agent-Y are in different parts of the Country-K.  
They are communicating via an in-secure channel.  
Agent-X sends an encrypted message(i.e cipher text) to Agent-Y.  
In the mid-way, Enemy and Agent-Y finds the cipher text but can’t able to understand.

Diagram

Description automatically generated

So to make Agent-Y understand, Agent-X sends the key along with cipher text.  
Now both the enemy and Agent-Y scans the cipher text, key and decrypts the message.

Now without transferring the key, Agent-Y must decrypt and understand the message.

Generator g must be the primitive root / element of the Prime Number p.

Xa 🡪 private key of Agent-X  
Ya 🡪 private key of Agent-Y

A 🡪 public key of Agent-X (shared to Agent-Y)  
B 🡪 public key of Agent-Y (shared to Agent-X)

S 🡪 shared key

Logo, company name

Description automatically generated

Diagram

Description automatically generated with medium confidence

**Since the A,B,g,p values are small, we calculated the exponent part.  
If these values are larger, then it is very difficult to calculate the exponent part.**

Now Agent Y knows the key, So after getting the cipher text he can encrypt the message and finds out the meaning.  
Enemy knows only the cipher text, so can’t able to derive the meaning.

**Using Diffie Hellman, we shared a secret key over an in-secure channel.**

# **Elgamal Cryptosystem**

Agent-X and Agent-Y are in different parts of the Country-X.  
They are communicating via an in-secure channel.  
Agent-Y sends an encrypted message(i.e cipher text Y1 and Y2) to Agent-X.  
In the mid-way, Enemy finds the cipher text but can’t able to understand.

Logo, company name

Description automatically generated with medium confidence

Now, Agent Y sends the cipher text (Y1 and Y2) to Agent-X.

A picture containing text

Description automatically generated

Graphical user interface, text, application

Description automatically generated  
Text

Description automatically generated

Text

Description automatically generated