Introduction to Cryptography Teachers' Guide

After Module-1

In your class ask your students to devise a method to decrypt the message just been encrypted using Scytale. Ask them to use the pencil to decrypt the cipher text by using pencil.

Please encourage your students to use the Caesar Cipher and then further use Scytale to achieve a higher degree of encryption.

Tell them Caesar Cipher is a shift/substitution cipher as it is obtained by shifting all the characters thrice in a cyclic way.

While interactively working with them let them propose some other ciphers.

After Module -2

Encourage the students to decrypt the given cipher text.

After Module-3

Ask your students to turn the text mentioned at the end of the last module into 1's and 0's. To reduce the bits you may encourage them to find out a bit which carry's no information.

After Module-4

Please tell them about XOR table.

P	0	0	1	1
K	0	1	0	1
P⊕K =C (Sender did it)	0	1	1	0

Ask them to devise a simple way to get 'P' row from 'C'.

After Module-5

Facilitate a debate that whether it's possible to share a key in public, so that eavesdropper can't get it. Hopefully, they won't be able to figure out a method to do so☺. Now with a question in their mind lead them to the next module.

After Module-6

Take up the first problem $2^x = 27 \bmod (29)$

Encourage them to do some guess work, which will not work hopefully. Lead them to the systematic way to find it out and it is to tabulate all the powers of 2 in mod (29) and then by table lookup we will be able to get x = 15. Tell them that to get x is time consuming when compared with raising the power of '7' in mod (29). Tell them that the bigger that value of prime the more would the process be time consuming.

Take up the second problem $7^y = 16 \bmod (29)$

Now similarly take up the second problem, make a similar **complete** table to get y = 5, 12, 19, 26. Let the students feel the difference between the two tables. The

first table has all the numbers from 1 to 28 while the second table contains only $1/4^{th}$ of them.

A worksheet has been provided as Annex-V to solve these two problems.

After Module-7

Play Alice and Bob

Encourage your students to practice some key exchange by using p = 89 and g = 30 with a and b = 10, 20, 18, 19 etc. etc. You may stage a play with the help of two students acting as Alice and Bob and rest of the class as Eve. But be sure that the selection of "a", "b" and the relevant calculation is privately done by them. I am also sending you a small computer program to you by which you can take the power of a number in mod (p), please see Annex-VI. In my presentation I have taken a = 1551 and b = 1231

About the Module Challenge

Now $A = g^a \bmod (p)$ and $B = g^b \bmod (p)$

And $A^b \bmod (p) = (g^a)^b \bmod (p)$ which is the same as $B^a \bmod (p) = (g^b)^a \bmod (p)$

Guide them to figure it out.