**SYNOPSIS**

1. **GROUP ID:** 27
2. **PROJECT TITLE:**

Demonstration of secure and insecure websites

1. **GUIDE:**

Prof. R. H. Jadhav

1. **TECHNICAL KEYWORDS:**

ICS, Web page, Web Server, HTTP, HTTPS

1. **PROBLEM STATEMENT:**

To demonstrate the difference between using secure websites and insecure websites and how insecure websites are prone to man-in-middle attack.

1. **ABSTRACT:**

When visitors to any web site request a page using a secure https:// connection, a broken padlock icon may appear in the web browser's location bar. Google Chrome displays: “Your connection to example.com is not secure. These resources can be viewed by others while in transit, and can be modified by an attacker to change the look of the page.”

HTTPS encryption protects the channel between the browser and the website visit, ensuring no one in the middle can tamper with the traffic or spy on data. Without that encryption, someone with access to router or ISP could intercept information sent to websites or inject malware into otherwise legitimate pages.

The system implements a packet capturing program. The socket is bound and then listened over for any network activity. User-agent and URL visited gets displayed.

1. **GOALS AND OBJECTIVES:**

* Increase Google ranking
* Improve Security
* Updated Browser Label
* Increase conversions
* Increase customer confidence

1. **RELEVANT MATHEMATICS ASSOCIATED WITH THE PROJECT:**

For both RSA and ElGamal (and other systems) it is useful to know about the congruence concept. Two integers a and bare said to be congruent modulo m (a positive integer, which is at least 2) written:

IMG_256

if a and b leave the same remainder when divided by m or that b-a is precisely divisible by m with a zero remainder. Here are some examples:

IMG_257

IMG_258

IMG_259

Note that we can always arrange the number on the right-hand side of congruence to be a number between 0 and (m-1) where m is the modulus. Thus, we could replace 23 by 10 in the last congruence. It is not very difficult to find the value for the "?" in the congruence below:

IMG_260

The idea for doing this is to compute the values of 5, 52, 54, 58 and so on. Modulo 19 and then use the binary representation of exponent (in this case 72) to help compute the answer. However, the problem of finding the value of k for which the congruence below is valid is much less straightforward:

IMG_261

The problem of finding k in a situation such as this is known as the discrete logarithm problem. When the modulus is very large, methods which are appreciably better than brute force are not currently known. The complexity of finding discrete logarithms (for many m, in particular, when m is prime) and many [other algorithms](http://www.dtc.umn.edu/~odlyzko/doc/algorithms.html) that have been used to try to design public key systems, is not fully understood. It turns out that some systems based on NP-complete problems have been "[broken](http://www.derf.net/knapsack/)" while other systems which depend on problems whose complexity is still not understood entirely seem to be holding their own. Next, we will give a clear discussion of the popular RSA system, which gets used as a security measure on the Internet.