Zero Knowledge Protocol using RSA Algorithm

Pranav Saudagar
BE student of Computer Engineering
Atharva College of Engineering
Mumbai, MH, India

Prasanna Patil
BE student of Computer Engineering
Atharva College of Engineering
Mumbai, MH, India

Jayant Bhalani
BE student of Computer Engineering
Atharva College of Engineering
Mumbai, MH, India

Shweta Sharma
Prof. of Computer Engineering
Atharva College of Engineering
Mumbai, MH, India

***Abstract*— Cryptography has been in use for age's right from Caesar's era to world war to this moment. These days it's used more often for authentication, than not. Zero-Knowledge Algorithm and RSA are used or authentication proposes. Zero Knowledge with RSA provides that extra edge necessary in authentication. It can be applied at the client side. The algorithm acts a firewall keeping out unauthorized user. It allows a party to prove that he/she has the necessary permissions (i.e. Credential) to access the content, without having to send over the value of the credential itself. The purpose of this kind of deployment is to make user login more confidential and authentication more safe than before.**

***Keywords*— ZKP; RSA; ASP; SQL; Z-RSA; MD5**

I. INTRODUCTION

Zero-Knowledge proof is a much popular concept utilized in many cryptography systems [8][11]. In this concept, 2 parties are involved, the prover A and the verifier B. Using this technique, it allows prover A to show that he has a credential (for example, a credit card number), without having to give B the exact number. The reason for the use of a Zero-Knowledge Proof in this situation for an authentication system is because it has the following properties:

- *Completeness:* If the statement is true, the honest verifier (that is, one following the protocol properly) will be able to prove that the statement is true to an honest verifier every time.
- *Soundness:* If the statement is false, it is not possible (with a very small chance) to fake the result to the verifier that the statement is true.
- *Zero-knowledge*: If the statement is true, the verifier will not know anything other than that the statement is true. Information about the details of the statement will not be revealed The formatter will need to create these components, incorporating the applicable criteria that follow.

II. LITERATURE REVIEW

According to Kota and Aissi, the RSA is a public key cryptographic algorithm that is used to help ensure data communication security. It is simply based on two main cryptographic processes [1]. First, using a public key it converts an input data called the plaintext into an unrecognizable encrypted output called cipher text (encryption process), such that it is impossible to recover the original plaintext without the encryption password in a reasonable amount of time. Second, using a private key, the RSA then converts the unrecognizable data back to its original form (decryption process)[3]. The algorithms used for public key cryptography are based on mathematical relationships (the ones being the integer factorization and discrete logarithm problems)[5].Although it is easy for the recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult for anyone to derive the private key, based only on their knowledge of the public key. This is why, unlike symmetric key algorithms, a public key algorithm does *not* require a secure initial exchange of one (or more) secret keys between the sender and receiver [2].

RSA algorithm:

- Select two different prime numbers p and q. For security aim, the integer's p and q must be prime numbers.
- Calculate n=p*q. n will be used as the module for public key and private key.
- Calculate f(n)=(q-1)(p-1), Where f is a function of Euler's
- Select an integer e such that 1<e<f(n) and GCD (e, f(n))=1; e and f(n) are co prime.
- Determine d: d is multiplicative inverse of e mod (f(n)) (e * d) mod f (n) = 1 d is the private key

Zero Knowledge Proof is really an intriguing and important applicative subject [8]. Zero Knowledge Proof has been in the sights of many cryptographic experts who have kept their eyes on its development over the years. It has potential to be used extensively in security fields.[10][11]. Zero Knowledge Proof essentially hides the actual credentials and works as if nothing is passed over and only authentication is provided.

Sole working of Zero Knowledge Proof in terms of authentication is depicted below

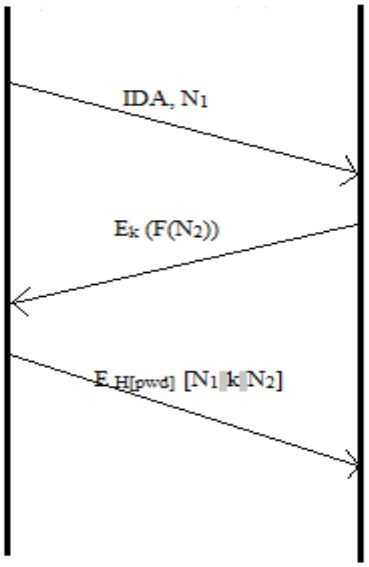

Fig. 2.1 Flow of Zero Knowledge Protocol

Notations:

- IDA; Username of 'A'
- N_1 and N_2; Nonce
- k; Shared secret key
- F; Transformation Function
- E_k; Encryption using shared Key
- H[pwd]; Password hash

III. METHODOLOGY

The process is divided in two phases:

- Login Phase
- Registration Phase

1) Login Phase

Each user having an unique number is necessary for the process to work. Every time new users enter/requests the login page, that person will initiate a process which will generate a unique number which will be saved in the database and carried forward. This number is added to the CRC hash in the password.

The algorithm is given below

- Request login page and token generation
- Password hashing using CRC32 checksum algorithm
- Password function is generated i.e. $Y=H(Pass)+g_o$. g_o is from public key list G
- User generates randomly r
- User calculates $T_1=g_o+r$
- User calculates $C=T_1+V+O$
- User calculates $z=r+C-Y$
- Sends C & z to server
- Server calculates $T_2=Y-C+g_o+z$. T_2 should be equal to T_1
- Server solves $e=T_2+Y+4$ & changes with C sort by user, should be same as T_2
- If yes, the user is verified

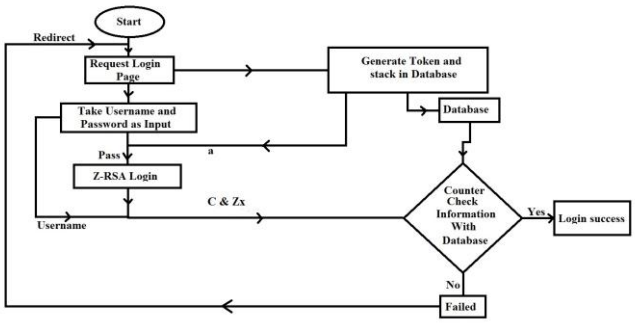

Fig. 2.2 Login Process for Z-RSA Algorithm

2) Registration Phase

Before anything the user has to register for the access. Here the user is prompted to enter his username and create a password. The password is encrypted using CRC32 algorithm. Then Y is generated and stored in Database.

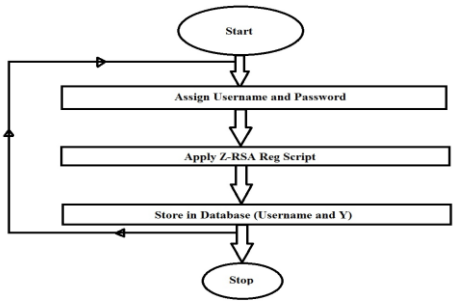

Fig. 2.3 Registration Process for Z-RSA Algorithm

Algorithm is as follows:-

- Register username and password
- Hash password with CRC32 algorithm
- $Y=H(pass)+g_o$
- Store it in database

FUTURE SCOPE

The immense rise in the use of web applications and web interface based mobile applications are the red flags for the possible outbreak of highly confidential data through a attacker monitoring the network. The recent iCloud hack which caused a havoc is enough to show us that. When there isn't actual transfer of credentials the attacker would be clueless about them. The proposed system can be used in places of high secrecy maintaining circumstances.

If further developed, this can also be used to secure chunks of data to transmit over the air.

CONCLUSION

In this paper we discussed the problems arising from the immense use of web based applications in mobile phones and other mediums, which lead us to the need of higher level of authentication. The proposed system uses a RSA to implement ZKP using random number generator for every login instance and the hash (stored in crc32) is added to it and the server counter checks the values for access granting

REFERENCES

[1] Implementation of the RSA algorithm and its cryptanalysis Chandra M. Kota and Cherif Aissi1 University of Louisiana at Lafayette, College of EngineeringLafayette, LA 70504, USA

[2] A Modified RSA Encryption Technique Based on Multiple public keys, Amare Anagaw Ayele Dr. Vuda SreenivasaraoM.Sc. (Computer Science), School of Computing and Electrical Engineering, IOT, Bahir Dar University, Ethiopia1 Professor, School of Computing and Electrical Engineering, IOT, Bahir Dar University, Ethiopia, India

[3] Data Encryption and Decryption Using RSA Algorithm in a Network Environment Nentawe Y. Goshwe. Department of Electrical/Electronics Engineering University of Agriculture, Makurdi

[4] Modified RSA Algorithm for (Wi-Fi) Security Protocol T.Venkata Satya Vivek, D.Anandam , Ganta Anil,B.Sreenivasulu, V.Lakshma Reddy, M Rao Batchnaboyina Computer Science And Engineering, PACE Institute of Technology & Sciences,Ongole, India

[5] Secure Communication using RSA Algorithm for Network Environment Amrita Jain Department of Information Technology IET DAVV, Indore (M.P), India Vivek Kapoor, Ph.D Department of Information Technology IET DAVV, Indore (M.P), India

[6] Study on Improvement In Rsa Algorithm and Its Implementation P.Saveetha & S.Arumugam Dept of IT, Nandha college of Technology, Erode

[7] A Study and Performance Analysis Of Rsa Algorithm M. Preetha, M. NithyaComputer Science & Application & Periyar University, India

[8] Zero knowledge protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System (Z-RSA) Vikash Mainanwal, Mansi Gupta, Shravan Kumar Upadhayay

[9] Lindell,Y;Zarosim,H.Adaptive Zero-knowledge Proofs and Adaptively Secure Oblivious Transfer.[J].Journal of Cryptology.24(4),pp.761-799,2011

[10] Garg,Sanjam;Jain,Abhishek;Sahai,Amit.Leakage-resilient zero knowledge.31st Annual International Cryptology Conference,CRYPTO 2011.pp:297-315.

[11] Lin,Huijia;Pass,Rafael;Tseng,Wei-Lung Dustin Venkitasubramaniam, Muthruamakrishnan. Concurrent non-malleable zero knowledge proofs. 30th Annual International Cryptology Conference,CRYPTO 2010.pp:429-446