**Authentication by Encrypted Negative Password Encrypted Using RSA Rule**

**ABSTRACT**:

Security is the fundamental angle for setting solid passwords for all our online media or any kind of records that are protected. The data which is given as an input are secured for privacy purpose, later it is hacked by the intruders. So for that reason, an outline called encoded negative password is proposed. After obtaining the secret phrase from the client, the password is hashed (Hashing the secret key by SHA). The hashing is scrambled to obtain the hashed secret key by utilizing two other calculations

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * WING to the development of the Internet, a vast number of online services have emerged, in which password authentication is the most widely used authentication technique, for it is available at a low cost and easy to deploy, Hence, password security always attracts great interest from academia and industry. Despite great research achievements on password security, passwords are still cracked since users’ careless behaviors. For instance, many users often select weak passwords; they tend to reuse same passwords in different systems; they usually set their passwords using familiar vocabulary for its convenience to remember. In addition, system problems may cause password compromises. It is very difficult to obtain passwords from high security systems. | * The proposed framework includes two phases: the registration phase and authentication phase. * When adopting our framework to protect passwords in an authentication data table, the system designer must first select a cryptographic hash function and a symmetric-key algorithm, where the condition that must be satisfied is that the size of the hash value of the selected cryptographic hash function is equal to the key size of the selected symmetric-key algorithm |
| **EXISTING ALGORITHM**  Advanced Encryption Standard (AES) | **PROPOSED ALGORITHM:-**  RSA Algorithm |
| **ALGORITHM DEFINITION:-**  AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.  The cryptographic hash work maps the informant ion of subjective size to a fixed-size grouping of pieces.  In the validation framework, it utilizes the hashed secret word plot, just as the hashed secret keys. Rainbow table assault is more useful for its space-time trade off. | **ALGORITHM DEFINITION:-**  The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names  suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.  The RSA algorithm ensures that the keys, in the above illustration, are as secure as possible. The following steps highlight how it works: |
| **DRAWBACKS: -**   * Plane password is the main password of profile. * Week security. * They tend to reuse same passwords in different systems | **ADVANTAGES: -**   * We propose a password protection scheme called ENP, and we propose two implementations of the ENP: ENPI and ENPII, including their generation algorithms and verification algorithms. Furthermore, a password authentication framework based on the ENP is presented. * We analyze and compare the attack complexity of hashed password, salted password, key stretching and the ENP. The results show that the ENP could resist lookup table attack without the need for extra elements and provide stronger password protection under dictionary attack. |

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS**:

System : Pentium i3 Processor

Hard Disk : 500 GB.

Monitor : 15’’ LED

Input Devices : Keyboard, Mouse

RAM : 2 GB

**SOFTWARE REQUIREMENTS:**

Operating system : Windows 10.

Coding Language : Java.

Tool : Eclipse

Database : MYSQL