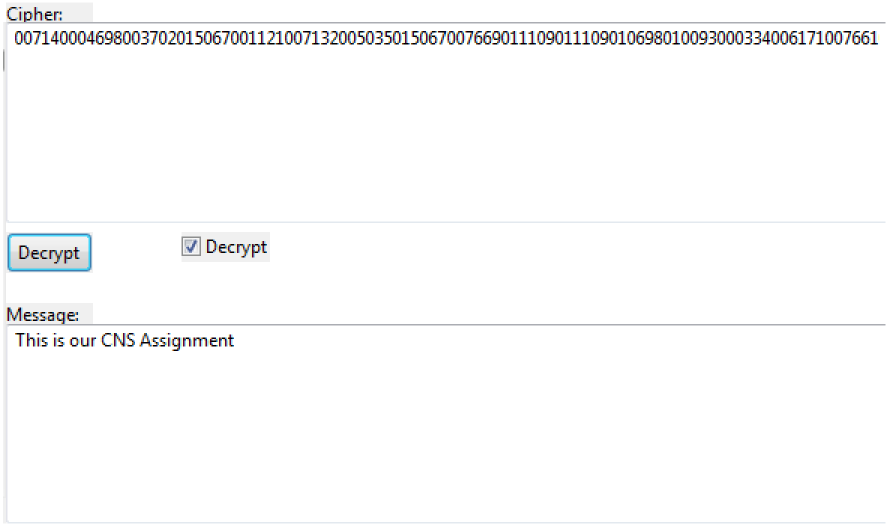
November 28, 2012

RV College of Engineering

Department of Computer Science



Cipher:
00714000469800370201506700112100713200503501506700766901110901110901069801009300033400617100 7661

Message:
This is our CNS Assignment

Schmidt-Samoa Cryptosystem

By:
Satvik N [1RV09CS095]
Vaishakh BN [1RV09CS114]

1 Introduction

Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. Neither key can perform both functions. One of these keys is published or public, while the other is kept private.

How Pubic-key Cryptosystems Work

The distinguishing technique used in public-key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys - a public encryption key and a private decryption key. The publicly available encrypting-key is distributed, while the private decrypting-key is kept secret. Messages are encrypted with the recipient's public key, and can be decrypted only with the corresponding private key. The keys are related mathematically, but the parameters are chosen so that determining the private key from the public key is either impossible or prohibitively expensive.

Schmidt-Samoa Public-key Cryptosystem

The Schmidt-Samoa cryptosystem is an asymmetric cryptographic technique, whose security, like Rabin and RSA depends on the difficulty of integer factorization.

- Key generation
  - Choose two large distinct primes p and q and compute $N = p^2 \times q$
  - Compute $d = N - 1 \text{ mod } lcm(p-1, q-1)$
  - Now N is the public key and d is the private key.
- **Encryption** - To encrypt a message m we compute the cipher text as $c = m^N modN$
- **Decryption** To decrypt a cipher text c we compute the plaintext as $m = c^d mod(p \times q)$ which like for Rabin and RSA can be computed with the Chinese remainder theorem.
- **Security** - The algorithm, like Rabin, is based on the difficulty of factoring the modulus N, which is a distinct advantage over RSA. That is, it can be shown that if there exists an algorithm that can decrypt arbitrary messages, then this algorithm can be used to factor N.

2 Previous Cryptosystems

RSA Cryptosystem

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1977.

- **Key Generation**
  - Let N = pq be a product of two prime numbers
  - Compute $(n) = (p1)(q1)$, where is Euler's totient function.

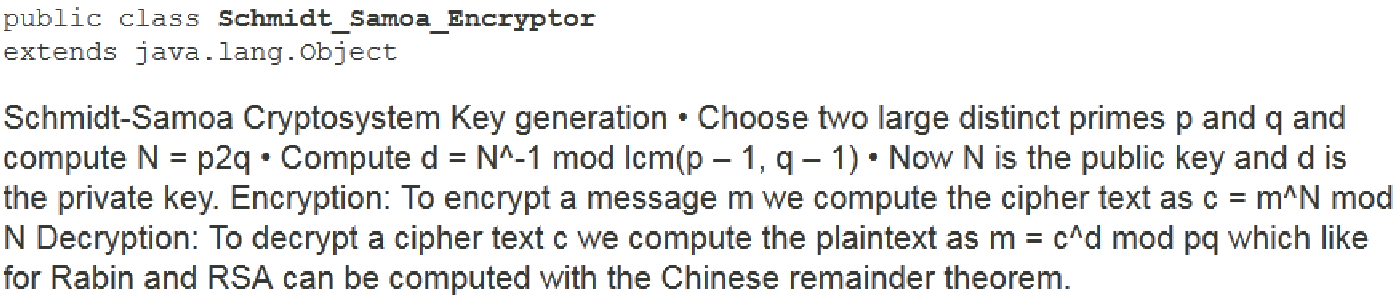
- Choose an integer e such that 1 ¡ e ¡ (n) and greatest common divisor of (e, (n)) = 1; i.e., e and (n) are coprime.
- Determine d as: d e-1 (mod (n)) i.e., d is the multiplicative inverse of e mod (n).

- **Encryption**: Let M be a message, and c the ciphertext. Then, $c = m^e (modn)$
- **Decryption**: $m = c^d (modn)$ By construction, d*e= 1 mod (n). The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret.

Rabins Cryptosystem

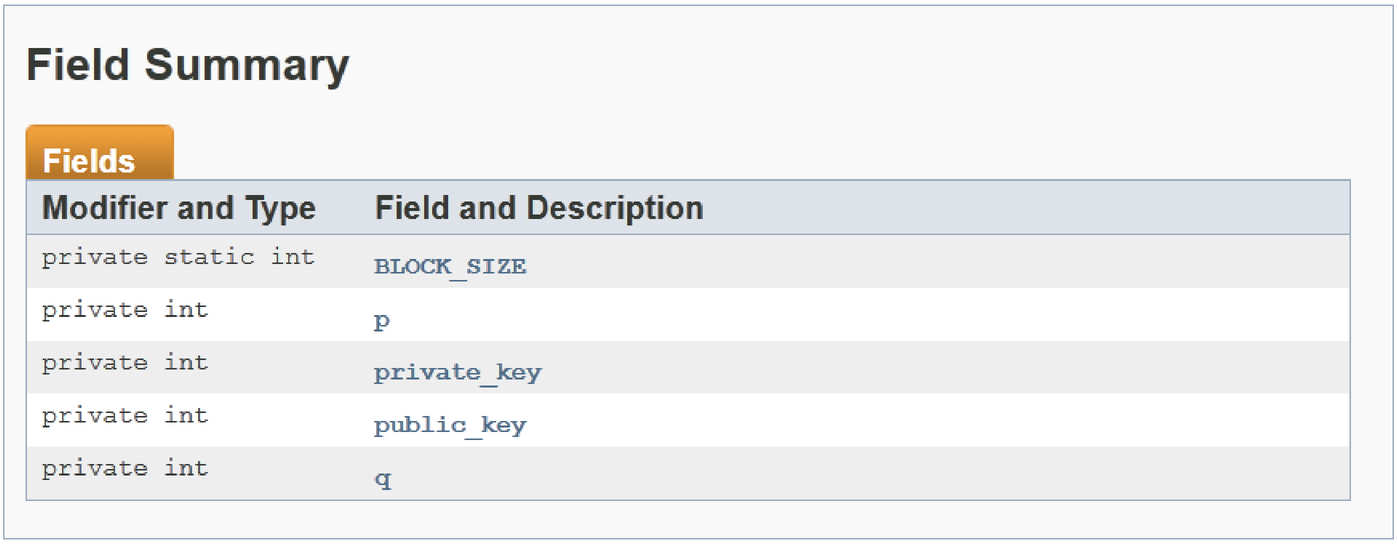
In 1979, Michael Rabin suggested a variant of RSA with public-key exponent 2, which he showed to be as secure as factoring. Let N = pq be a product of two prime numbers. Encryption. Let m ZNx, M be a message, the encryption is C = m2 mod N Decryption. To decrypt we solve the equation x2 = C mod N which has four roots in ZNx

3 Implementation



```
public class Schmidt_Samoa_Encryptor
extends java.lang.Object
```

Schmidt-Samoa Cryptosystem Key generation • Choose two large distinct primes p and q and compute N = p2q • Compute d = N^-1 mod lcm(p – 1, q – 1) • Now N is the public key and d is the private key. Encryption: To encrypt a message m we compute the cipher text as c = m^N mod N Decryption: To decrypt a cipher text c we compute the plaintext as m = c^d mod pq which like for Rabin and RSA can be computed with the Chinese remainder theorem.

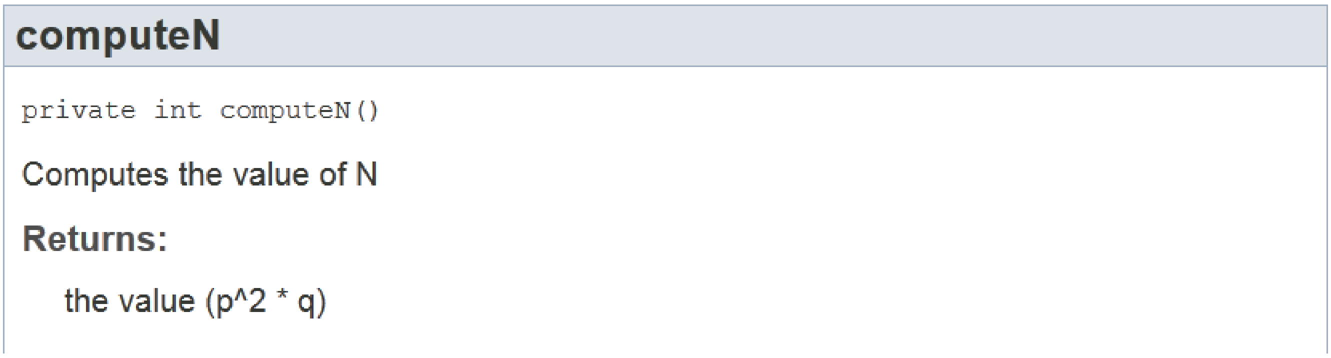


Field Summary

Fields

Modifier and Type	Field and Description
private static int	BLOCK_SIZE
private int	p
private int	private_key
private int	public_key
private int	q

Figure 1: Experimental Results



computeN

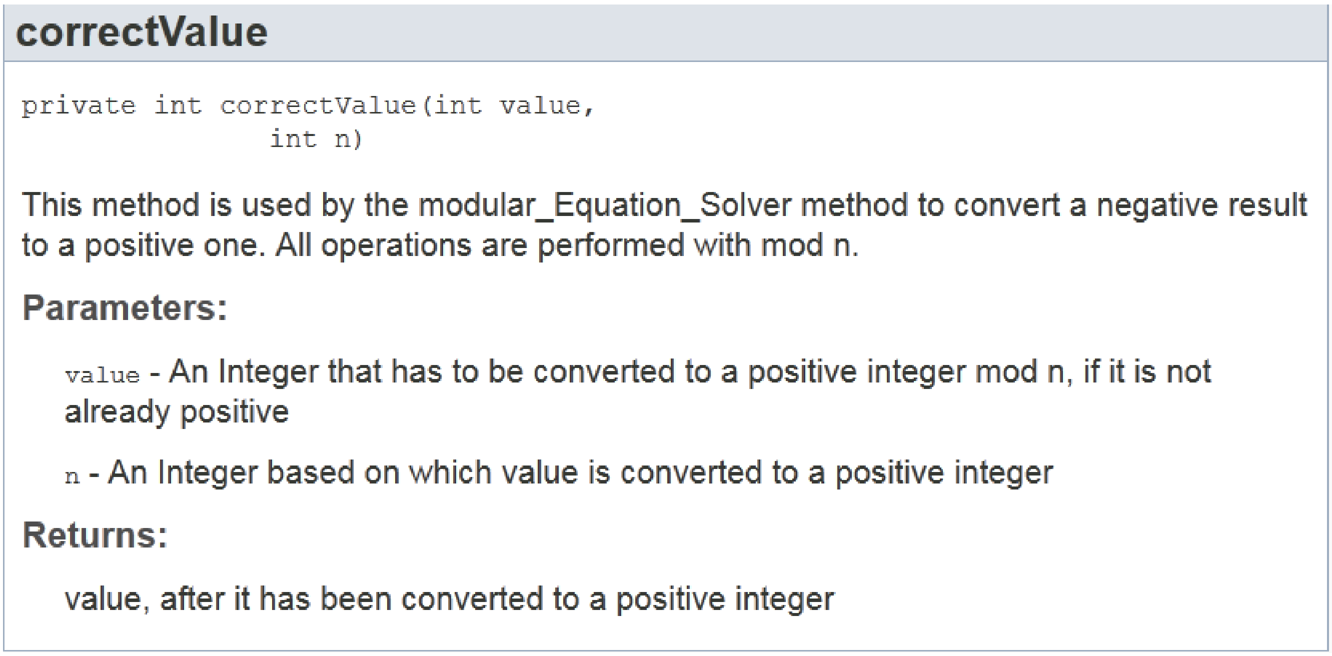
```
private int computeN()
```

Computes the value of N

Returns:

the value (p^2 * q)

Figure 2: Experimental Results



correctValue

```
private int correctValue(int value,
                         int n)
```

This method is used by the modular_Equation_Solver method to convert a negative result to a positive one. All operations are performed with mod n.

Parameters:

`value` - An Integer that has to be converted to a positive integer mod n, if it is not already positive

`n` - An Integer based on which value is converted to a positive integer

Returns:

value, after it has been converted to a positive integer

Figure 3: Experimental Results

References

[1] Katja Schmidt-Samoa, *A New Rabin-type Trapdoor Permutation Equivalent to Factoring and Its Applications*. TechnischeUniversit. samoa@informatik.tu-darmstadt.de

[2] Schmidt-Samoa Cryptosystem - `http://en.wikipedia.org/wiki/Schmidt-Samoa_cryptosystem`

[3] Rivest, R.; A. Shamir; L. Adleman (1978). *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"*. Communications of the ACM 21 (2): 120126. doi:10.1145/359340.359342

[4] Joe Hurd, Blum Integers (1997) - `http://www.gilith.com/research/talks/cambridge1997.pdf`

[5] Rabin, Michael. *Digitalized Signatures and Public-Key Functions as Intractable as Factorization.* MIT Laboratory for Computer Science, January 1979.

[6] Katja Schmidt-Samoa - *Contributions to Provable Security and Efficient Cryptography.* `http://tuprints.ulb.tu-darmstadt.de/708/1/Diss.Schmidt-Samoa.pdf`

4 Screenshots

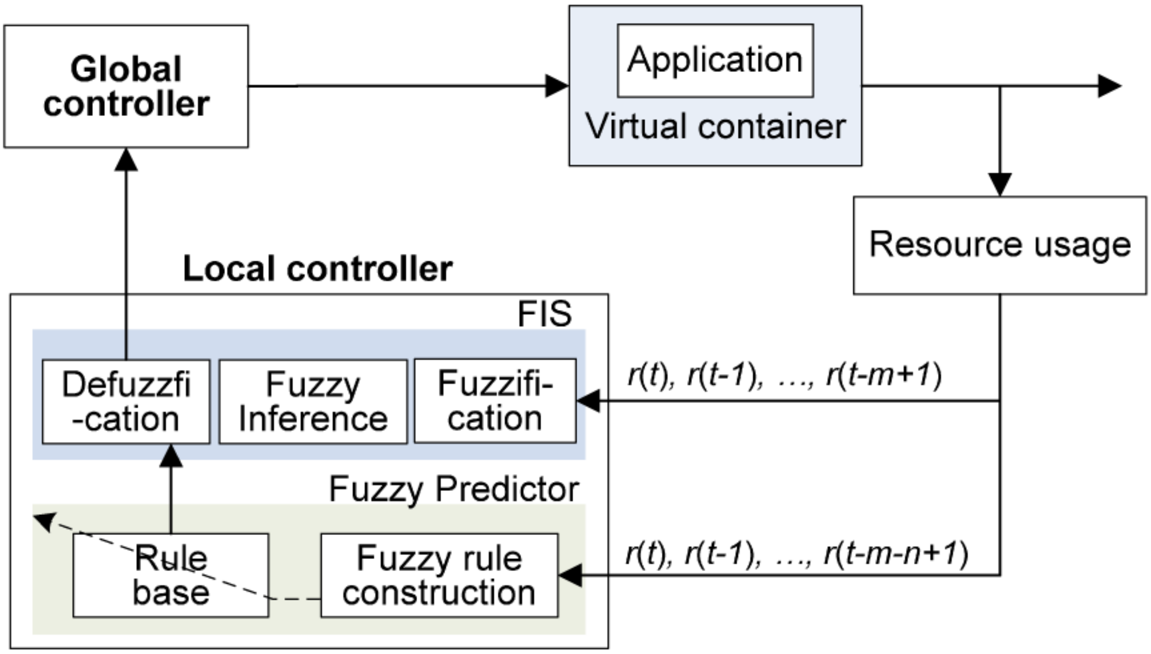


Figure 4: Resource management based on fuzzy logic systems.

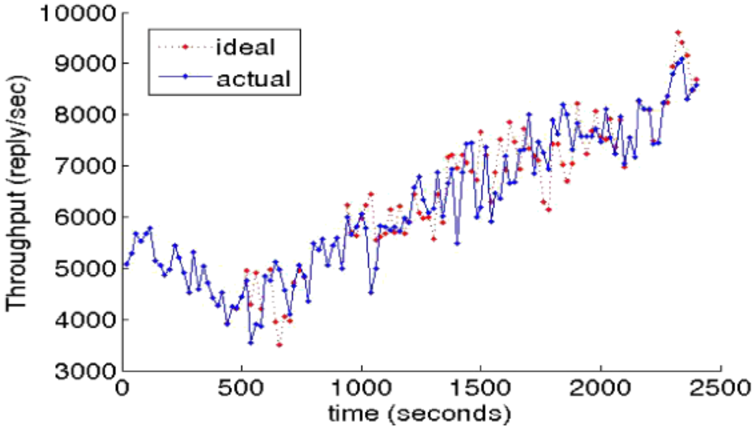


Figure 5: Experimental Results

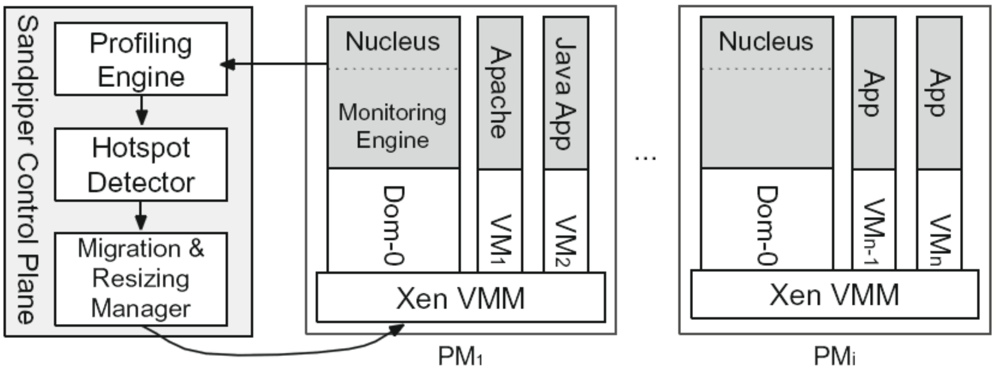


Figure 6: The Sandpiper architecture.