

# A hybrid cryptographic system for file security

*Presented by:* Group-H

Dept. Of Computer Science and Engineering  
Tripura Institute of Technology, Narsingarh



## Team Members:

- Hamjak Debbarma [27/CS/L/23/47]
- Joydeep Saha [27/CS/L/23/56]
- Raju Debnath [27/CS/23/12]

**Supervised By:** Prof. Pankaj Debbarma

- Problem Statement
- Solution
- Hybrid Cryptography
- RSA Algorithm
- KASUMI Cipher
- Proposed System Design
- Advantages of Proposed System
- Implementation
- Further Work
- References

# Problem Statement

- In this information and digital age, we generate a lots of data
- Many personal documents and important business files are shared across all over the internet
- All these are vulnerable to attack and information breaches.

The solution is to build secure encryption system using the secure cryptographic algorithms that could withstand various attacks.

# Hybrid Cryptography

The ISO/IEC JTC1/SC27 standardization committee suggests that hybrid cryptography can be defined as the branch of asymmetric cryptography that makes use of convenient symmetric techniques to remove some of the problems inherent in normal asymmetric cryptosystem.

**Hybrid Cryptography** is the combination of both the symmetric key cryptography and Asymmetric or Public key cryptography.

# Hybrid Cryptography

Our Goal: to build a hybrid cryptosystem using the following algorithms:

- RSA Algorithm (Asymmetric)
- KASUMI Cipher (Symmetric)



# RSA Algorithm

- Public Key Cryptosystem
- Invented by Rivest, Shamir and Adleman [1977]
- It is based on the principle that it is easy to multiply large numbers but factoring large number is very difficult.
- Public key is generated by multiplying two large prime numbers and private key is generated by using a mathematical functions.
- Key Size : 512 bits to 4096 bits

# RSA: Advantages

- RSA Algorithm involves a lot of complex mathematics which makes it more difficult to crack.
- Fast Encryption as compare to other encryption algorithm.
- No need of sharing secrets key
- Proof of owner's authenticity
- Data cannot be modified at transit

# RSA: Disadvantages

- Key generation is very slow.
- Speed of encrypting of text is slow.
- High processing is required at receiver's end for decryption

# KASUMI Cipher

- It is a Feistel Cipher
- Based on the MISTY1 Cipher
- Mostly used in Universal Mobile Telecomm. System(UMTS), Global System for Mobile Comm. (GSM) and GPRS Mobile Comm.
- Key size: 128 bits
- Block Size: 64 bits
- The core of KASUMI is an 8-round Feistel network.
- In each round the round function uses a round key which consists of eight 16-bit sub keys derived from the original 128-bit key using a fixed key schedule.

**Working of Round Function:** Let's consider key,  $K$  is 32 bit and is divided into eight 4 bit values  $K_1, K_2, \dots, K_8$  i.e.,

$$K = K_1 || K_2 || \dots || K_8$$

Take  $k = 0111$  then subkeys :

$$K_1 = 0111$$

$$K_2 = 1011$$

$$K_3 = 1101$$

$$K_4 = 1110$$

$$K_5 = 0111$$

$$K_6 = 1011$$

$$K_7 = 1101$$

$$K_8 = 1110$$

where,  $K_1 = K_5$ ,  $K_2 = K_6$ ,  $K_3 = K_7$  and  $K_4 = K_8$

In KASUMI, round keys are :

$$KL_{i,1} = \text{ROL}(K_i, 1)$$

$$KL_{i,2} = K'_{i+2}$$

$$KO_{i,1} = \text{ROL}(K_{i+1}, 5)$$

$$KO_{i,2} = \text{ROL}(K_{i+5}, 8)$$

$$KO_{i,3} = \text{ROL}(K_{i+6}, 13)$$

$$Kl_{i,1} = K'_{i+4}$$

$$Kl_{i,2} = K'_{i+3}$$

$$Kl_{i,3} = K'_{i+7}$$

Round	$KL_{i,1}$	$KL_{i,2}$	$KO_{i,1}$	$KO_{i,2}$	$KO_{i,3}$	$KI_{i,1}$	$KI_{i,2}$	$KI_{i,3}$
1	$K_1 \lll 1$	$K'_3$	$K_2 \lll 5$	$K_2 \lll 8$	$K_3 \lll 13$	$K'_1$	$K'_4$	$K'_8$
2	$K_2 \lll 1$	$K'_4$	$K_3 \lll 5$	$K_3 \lll 8$	$K_4 \lll 13$	$K'_2$	$K'_1$	$K'_1$
3	$K_3 \lll 1$	$K'_1$	$K_4 \lll 5$	$K_4 \lll 8$	$K_1 \lll 13$	$K'_3$	$K'_2$	$K'_2$
4	$K_4 \lll 1$	$K'_2$	$K_1 \lll 5$	$K_1 \lll 8$	$K_2 \lll 13$	$K'_4$	$K'_3$	$K'_3$
5	$K_1 \lll 1$	$K'_3$	$K_2 \lll 5$	$K_2 \lll 8$	$K_3 \lll 13$	$K'_1$	$K'_4$	$K'_4$
6	$K_2 \lll 1$	$K'_4$	$K_3 \lll 5$	$K_3 \lll 8$	$K_4 \lll 13$	$K'_2$	$K'_5$	$K'_5$
7	$K_3 \lll 1$	$K'_1$	$K_4 \lll 5$	$K_4 \lll 8$	$K_1 \lll 13$	$K'_3$	$K'_6$	$K'_6$
8	$K_4 \lll 1$	$K'_2$	$K_1 \lll 5$	$K_1 \lll 8$	$K_2 \lll 13$	$K'_4$	$K'_7$	$K'_7$

Table 1: Round subkeys

# KASUMI: Advantages and Disadvantages

## Advantages:

- High diffusion and strong tamper resistance without detection
- More secure as compare to MISTY1

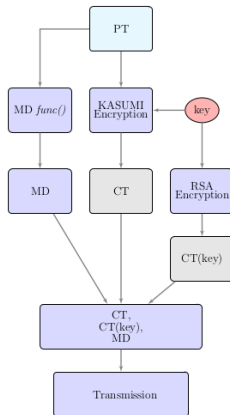
## Disadvantages:

- An impossible differential attack[1] on six rounds of KASUMI was presented by Kühn [2001]
- A related-key rectangle (boomerang) attack[2] on KASUMI that can break all 8 rounds faster than exhaustive search was published by Eli Biham, Orr Dunkelman and Nathan Keller[2005]



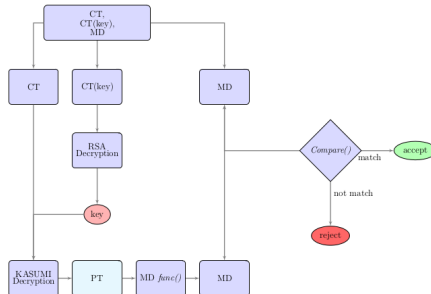
# Proposed System Design: Encryption

## Encryption Process



# Proposed System Design: Decryption

Decryption Process



# Advantages of proposed system

- File is secure as the file is being encrypted not by just using one but two highly algorithms RSA and KASUMI.
- The key used for encryption is also safe as it is encrypted by RSA
- Confidentiality and integrity of a file is being maintain securely as Hasing algorithm is used for generating checksum

# Implementation

For the proof of concept and for the demonstration we will be considering:

- Key Size: 32-bit instead of 128-bit
- Block Size: 16-bit instead of 64-bit

**Technologies used:** PHP and SQL

- Improving the Fiestel Round of the KASUMI Cipher for better security
- Introduction of another secret key to be used along with MD Function for maximum security.

- [1] Kühn, Ulrich. Cryptanalysis of Reduced Round MISTY. EUROCRYPT 2001.
- [2] Orr Dunkelman, Nathan Keller, Adi Shamir (2010-01-10). "A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony"
- [3] <https://en.wikipedia.org/wiki/KASUMI>

Thank You !