A refutation of "An efficient mixed mode and paired cipher text cryptographic algorithm for effective key distribution" by Rasmi P S and Varghese Paul

Nick Werline

Department of Electrical and Computer Engineering, University of Alabama in Huntsville

December 5, 2016

This paper disproves, by way of counterexample, the validity of the efficient mixed mode and paired cipher text cryptographic algorithm for effective key distribution proposed by Rasmi P S[*] and Varghese Paul[†].

Contents

[*]Department of Information Technology, TIST, Kochi, India

[†]CS/IT/Research, TIST, Kochi, India

1 Introduction

The algorithm proposed by Rasmi P S and Varghese Paul[1] was designed to be a cryptographic system that cannot be compromised as easily as other common methods employed today, such as the elliptical curve, ElGamal, Rabin, and RSA systems. Their mixed mode algorithm bases its security off of a combination of three "hard" mathematical problems. This makes the algorithm immune to future improvements to the solving of any one or two mathematical methods used. Their system employs the factoring, discrete logarithmic, and hidden root problems.

However, there is an error in the algorithm that does not always produce the expected result. This paper will provide counterexamples, following their methodology, that produce incorrect outcomes.

All further references to "the paper" are referring to [1].

2 Proof Analysis

2.1 Variable Selection

By using the key generation steps presented in the paper, the following variables are selected.

- Select two prime numbers, p and q where $p \neq q$ [*]

  $p = 5$

  $q = 17$

- Calculate $n = p \times q$

  $n = 85$

- Generate two random numbers S_a and S_b ($S_a < n$ and $S_b < n$)

  $S_a = 17$

  $S_b = 46$

- Select a number M corresponding to a letter of the alphabet ($1 \leq M \geq 27$) [†]

  $M = 5$

2.2 Theorem Calculation

In the published paper, Theorem 2 states:

$$(C_h^d \bmod n - S_b)/S_a = M \text{ if } C_h = (S_a \times M + S_b)^e \bmod n$$

[*] The paper expects the prime numbers to be very large in practice. However, small numbers are chosen here for clarity and follow closely to an example given by the authors: the prime numbers 3 and 11.

[†] 27 corresponds to a space

The proof continues to the step

$$M = ((S_a \times M + S_b) \bmod n - S_b)/S_a \text{ (use Fermat's little theorem)}^*$$

Filling in the numbers chosen in Section 2.1 produces

$$\begin{aligned}
5 &= ((17 \times 5 + 46) \bmod 85 - 46)/17 && (1)\\
&= (131 \bmod 85 - 46)/17 && (2)\\
&= (46 - 46)/17 && (3)\\
&= 0/17 && (4)\\
&\neq 0 && (5)
\end{aligned}$$

The LHS is not equivalent to the RHS and so Theorem 2 is not true.

3 Algorithm Analysis

3.1 Key generation

In the paper's section 4.4 *Numerical examples*, the authors provide an example encryption and decryption resulting in the following key generation

$$\text{Public key} = (e, r, n), \text{ private key} = (d, s, n), \text{ symmetric key} = (S_a, S_b)$$

where

$$\text{Public key} = (3,\ 1,\ 33), \text{ private key} = (7,\ 4,\ 33), \text{ symmetric key} = (3,\ 2)$$

As the selection criteria for S_a and S_b was

$$\text{Generate two random numbers } S_a \text{ and } S_b\ (S_a < n \text{ and } S_b < n)$$

For the counterexample, S_a and S_b will be modified from 3 and 2 to 11 and 3, respectively, to give the new key

$$\text{Public key} = (3,\ 1,\ 33), \text{ private key} = (7,\ 4,\ 33), \text{ symmetric key} = (11,\ 3)$$

*The paper actually excludes the outermost parenthesis here. However, it is assumed they were meant to be included based upon previous steps in the proof. Regardless, the inclusion or exclusion of these parenthesis does not affect the correctness of the end result.

3.2 Encryption

Continuing to follow the example given in the paper, the encryption is calculated as follows

1. $K = 7$
2. $M = 8$
3. $C_h = (11 \times 8 + 3)^3 \bmod 33 = 91^3 \bmod 33 = 16$ *
4. $C_f = (16)^3 \bmod 33 - 1^7 \bmod 33 = 4 - 1 = 3$ †
5. $C_s = 10^7 (\mathrm{mod} 33) = 10$
6. Cipher text $C = (3, 10)$ ‡

3.3 Decryption

1. $C_h = (3 + 10^4)^7 \bmod 33 = 16$
2. $M = (16^7 \bmod 33 - 3)/11 = (25 - 3)/11 = 22/11 = 2$

3.4 Comparison

As seen here, the final M value of 2 is not equivalent to the starting value of 8. The example used the same parameters as the paper, save for S_a and S_b being modified according to their selection rules.

4 Conclusion

The algorithm proposed by Rasmi P S and Varghese Paul in "An efficient mixed mode and paired cipher text cryptographic algorithm for effective key distribution" does not work as described for all values. This was proved by providing two counterexamples. These examples followed the algorithm's guidelines but failed to prove the stated Theorem 2 and failed to encrypt and decrypt successfully.

References

[1] Rasmi P S and Varghese Paul, *An efficient mixed mod and paired cipher text cryptographic algorithm for effective key distribution* in International Journal of Communication Systems, December 20, 2012, DOI: 10.1002/dac.2491

*In its corresponding step, the paper writes $3 \times 7 + 2 = 26$. The 7 is assumed to be a typo because $M = 8$ was declared just prior.

†The authors write $14 - 1 = 3$ here. It is assumed the correct equation should be $14 - 1 = 13$ because 13 is used later in their example.

‡The authors again write 3 at this step when 13 is expected because it is consistent with their following steps.