Journal of Computer Science 3 (6): 406-409, 2007
ISSN 1549-3636
© 2007 Science Publications

A Different Text Attack Algorithm in Integer Factoring Based Schemes

Mohammed A AL-Fayoumi, Sattar J Aboud and Musbah M. Aqel
Middle East University for Graduate Studies, Faculty of IT
Department of Computer Information Systems, Amman - Jordan

Abstract: Text attack in integer factoring based schemes is generally calculated as an intrinsic characteristic of its symmetric attack. In this article, we illustrate that asymmetric integer factoring based schemes are also vulnerable to a text attack. Also, we show that a single message is required to increase a successful text attack versus the Lucas scheme.

Key words: Integer factoring schemes, RSA scheme, Lucas scheme, text attack.

INTRODUCTION

The widely employed public key encryption schemes now base their security on the difficulty of the integer factoring problems such as the RSA scheme[1]. Its security based on the difficulty of factoring a modulus which is the product of two large primes. On account of its reputation, the RSA scheme is liable to considerable attacks. Various attacks are relied on the multiplicative inverse[2-4]. To conquer this weakness, many ideas are suggested and defeated. Other methods are considered to apply analogues of RSA. This is being the right technique to break the symmetric attack. Thus, encryption relied on Lucas sequences is suggested[5-6]. In this article, we use the Lucas sequences[7-8] to construct the proposed scheme. The Lucas scheme is being intractable versus symmetric attack. Though, the availability of a message forgery that requires two messages[9]. In this article, we introduce a novel text attack algorithm that requires a single message. The proposed attack algorithm illustrate that the integer factoring based schemes are similar to RSA scheme. This means that all attacks are relied on the multiplicative inverse of the RSA scheme and can easily be modified to any RSA based scheme.

Lucas type RSA scheme: we introduce a scheme that relied on Lucas sequences[8]. However, the Lucas scheme can be described as follows. Entity A selects two prime numbers p and q and a public key e which is co-prime to $(p^2-1)(q^2-1)$, then calculates $n = p*q$ and determined (n, e) as a public key. Then compute the secret key $d \equiv e^{-1} \bmod lcm(p-1, p+1, q-1, q+1)$. So, A 's public key is $(n \ , e)$ while A 's private key is p, q and d . The message m is encrypted by finding $w \equiv v_e(m,1) \bmod n$; it recovers employing the private key d using $m \equiv v_d(w,1) \bmod n$. The rightness of this scheme is relied on theorem 1 in the next section as $v_d(v_e(m,1) \equiv v_{d*e}(m,1) \equiv v_1(m,1) \equiv m \bmod n$. The signature is generated correspondingly by swapping the tasks of the public and private keys e and d .

Lucas System: Suppose p, q are both integer numbers, $z = p^2 - 4*q$ is a non-square, $g = \frac{p+\sqrt{z}}{2}$ and $s = \overline{g} = \frac{p-\sqrt{z}}{2}$ is the root of $r^2 - p*x + q = 0$ in the quadratic residue $_{q(\sqrt{z})}$. The Lucas sequences $v_i(p,q)$ and $u_i(p,q)$ for $i \in Z$ are then determined as the integers achieving by the following equation:

$$g^i = \frac{v_i(p,q)}{2} + \frac{u_i(p,q)\sqrt{z}}{2} \tag{1}$$

Thus $g^2 = p*g - q$ and $g^i = p*g^{i-1} - q* \ g^{i-3}$, then the Lucas sequences meet the following recurrence function.

$$v_0(p,q) = 2;$$
$$v_1(p,q) = p; \ v_i(p,q) = p*v_{i-1}(p,q) - q*v_{i-2}(p,q);$$
$$u_0(p,q) = 0;$$
$$u_1(p,q) = 1; \ u_i(p,q) = p*u_{i-1}(p,q) - q*u_{i-2}(p,q)$$

The recurrence function in certain times is employed as another definition of Lucas sequences. As long as multiplication is swappable it tracks that:

Corresponding Author: Mohammed A. AL-Fayoumi, Middle East University for Graduate Studies Faculty of IT Department of Computer Information Systems, Amman - Jordan

$$s^i = \overline{g}^i = \frac{v_i(p,q)}{2} - \frac{u_i(p,q)\sqrt{z}}{2}$$

From this formula and from formula (1) it tracks that:

$$v_i(p,q) = g^i + s^i \qquad (2)$$

And $u_i(p,q) = \dfrac{g^i - s^i}{g - s}$ (3)

Theorem 1: This theorem contains certain public characteristics of Lucas sequences

$$4q^i = v_i(p,q)^2 - z*u_i(p,q)^2 \qquad (4)$$

$$v_{i*m}(p,q) = v_i(v_m(p,q), q^m) \qquad (5)$$

$$u_{i*m}(p,q) = u_m(p,q)u_i(v_m(p,q), q^m) \qquad (6)$$

$$v_{i+m}(p,q) = \frac{v_i(p,q)v_m(p,q)}{2} + \frac{z*u_i(p,q)u_m(p,q)}{2} \qquad (7)$$

$$u_{i+i}(p,q) = \frac{u_i(p,q)v_m(p,q)}{2} + \frac{v_i(p,q)u_m(p,q)}{2} \qquad (8)$$

Proof 1: formula (4) can be proofs as follows:

$$4*q^i = 4(g*\overline{g})^i = 2*g^i*2*\overline{g^i}$$
$$= (v_i(p,q) + u_i(p,q)\sqrt{z})\ (v_i(p,q) - u_i(p,q)\sqrt{z})$$
$$= v_i(p,q)^2 - z*u_i(p,q)^2$$

Formula (4) now involves that:

$$g^i = \frac{v_i(p,q)}{2} + \frac{u_i(p,q)\sqrt{z}}{2} = \frac{v_i(p,q)}{2} + \frac{\sqrt{u_i(p,q)^2*z}}{2}$$
$$= \frac{v_i(p,q)}{2} + \frac{\sqrt{v_i(p,q)^2 - 4*q^i}}{2}$$

And since $g^i = p^{-}/2 + \sqrt{p^{-^2} - 4*q^{-}/2}$

With $p^{-} = v_i(p,q)$ and $q^{-} = q^i$. So we have

$$(g^i)^m = \frac{v_m(p^{-},q^{-})}{2} + \frac{u_m(p^{-},q^{-})\sqrt{p^{-^2} - 4*q^{-}}}{2}$$
$$= \frac{v_m(p^{-},q^{-}}{2} + \frac{u_m(p^{-},q^{-})u_i(p,q)\sqrt{z}}{2}$$

Evaluating the coefficients of this formula with

$$g^{i*m} = v_{i*m}(p,q)/2 + u_{i*m}(p,q)\sqrt{z/2}$$

Proofs: formulas (5) and (6). Finding $g^{i+m} = g^i * g^m$ as total of Lucas sequences and evaluating the coefficients demonstrates formulas (7) and (8).

Theorem 2: Suppose p is a prime number $q = 1$, and $\gcd(z,p) = 1$. So the sequence $v_i(p,1) \bmod p$ is cyclic and the size of the cycle divides $p - \left(\frac{z}{p}\right)$.

Proof 2: g and then also g^p are algebraic integers in $q(\sqrt{z})$. So we have $a^p = (p/2 + \sqrt{z}/2)^p \equiv p/2 + (\sqrt{z})^p/2 \equiv p/2 + z^{(p-1)/2} * \sqrt{z}/2 \equiv p/2 + \left(\frac{z}{p}\right) * \sqrt{z}/2 \bmod p$. So if $\left(\frac{z}{p}\right) = 1$ then $g^{p-1} \equiv 1 \bmod p$ and if $\left(\frac{z}{p}\right) = -1$ then g^{P+1} it follows that the sequence g^i and also $v_i(p,1)$ is cyclic with a cycle that divides $p - \left(\frac{z}{p}\right)$

The proposed scheme: Assume $n = p*q$ is composite modulus. Suppose e and d are the public key and the private key of entity A respectively, corresponding to $e*d \equiv 1 \bmod \theta(n)$. The exponent key e is employed to encrypt message and also for signature verifications; the private key d is employed to recover message and to sign messages. Assume an attacker Oscar desires to let entity A to sign the message m without authorization. Oscar can attack as follows. First select an arbitrary integer number i and lets entity A to sign or to recover $m^{-} \equiv m*i^e \bmod n$. Oscar then obtains $w^{-} \equiv m^d(i^e)^d \equiv m^d * i$ and then the signature w of message m as $w \equiv w^{-} * i^{-1} \bmod n$. As a result, message attacks versus the composite modulus appear fairly in nature is a result of its multiplicative inverse. Through re-expressing this attack with the extended Euclidean method, it seems that asymmetric schemes are also vulnerable to an attack. Employing the RSA scheme the attack works as follows:

* Oscar selects an integer number i co-prime to e. Then utilizes the extended Euclidean method to obtain $j,a \in Z$ where $i*j+e*\ a = 1$

* Oscar finds $m^{-} \equiv m^i \bmod n$

* Then, Oscar inquires Alice to sign m^{-} and obtains $w^{-} \equiv m^{-d} \bmod n$

* Thus Oscar can calculate the signature w as follows: $w \equiv w^{-j} * m^a \bmod n$ (9)

Proof: If $i*j+e*a=1$, then $d = d(i*j+e*a) \equiv d*i*j + a \bmod \theta(n)$

Lucas type scheme attack: The former attack is appropriate also for asymmetric schemes. In this section, we illustrate its mechanism versus Lucas type scheme. The attacker Oscar can attempt to obtain a signature w on a message m as follows.

* Oscar selects an integer number i co-prime to e. Then utilize the extended Euclidean method to obtain $j,a \in Z$ where $i*j+e*\ a = 1$.

* Oscar finds $m^{-} \equiv v_k(m,1) \bmod n$

* Then Oscar asks Alice to sign m^{-}. If Alice signed then Oscar will knows w^{-} where $w^{-} \equiv v_d(m^{-},1) \bmod n$

* Now Oscar finds the signature w of m as follows

$$v_{j*i*d}(m,1) \equiv v_j(w^{-},1) \bmod n \tag{10}$$

$$u_{j*i*i}(m,1) \equiv \frac{u_i(m,1)u_j(w^{-},1)}{u_e(w^{-},1)} \bmod n \tag{11}$$

$$w = v_d(m,1) \equiv \frac{v_{j*i*d}(m,1)v_s(m,1)}{2} + \frac{z * u_{j*i*d}(m,1)u_s(m,1)}{2} \bmod n \tag{12}$$

Such that $z = m^2 - 4$. Formula (10) results from formula (5).Since $v_3(w^{-},1) \equiv v_3(v_{i*d}(m,1),1) \equiv v_{j*i*d}(m,1)$ mod n

Formula (11) is a result of formula (6) since

$$u_{j*i*d}(m,1)v_e(w^{-},1)$$
$$\equiv u_j(v_{i*d}(m,1),1)u_{i*d}(m,1)u_e(v_{i*d}(m,1),1)$$
$$\equiv u_j(v_{i*d}(m,1),1)u_{i*d*e}(m,1)$$
$$\equiv u_j(v_{i*d}(m,1),1)u_i(m,1) \bmod n$$

Furthermore, $i * j + e * a = 1$ involves

$$v_d(m,1) = v_{j*i*d+d*e*a}(m,1) = v_{j*i*d+a}(m,1) .$$

Therefore Formula (12) is a reference of formula (7). Notice that this attack is an analogue to the message attack on composite modulus introduced in former section, by employing algebraic numbers replace m by $g = m + \sqrt{z/2}$ and employ formula (1). The only extra step can be verify is that $u_{i*d}(m,1)$ is calculable from m and $v_{i*d}(m,1)$. This can be illustrated by employing formula (6) and noticing that, $u_i(m,1) \equiv u_{i*d*e}(m,1) \equiv u_{i*d}(m,1)\ u_e(v_{i*d}(m,1),1) \bmod n$. If $g = m/2 + \sqrt{z/2}$. Then a signature $v_{i*d}(m,1)$ on the message $v_i(m,1)$ is employed to find $g^{i*d} \equiv v_{i*d}(m,1)/2 + u_{i*d}(m,1) \sqrt{z/2}$. After g^{i*d} is accepted $g^d = v_d(m,1)/2 + v_d(m,1) \sqrt{z/2}$ obtain as follows $g^d \equiv g^{(i*r+e*a)d} \equiv (g^{i*d})^j * g^a \bmod n$. Therefore formula (10) and formula (11) corresponds to the calculation of w^{-j} and formula (12) corresponds to the multiplication of w^{-j} by m^a in formula (9).

General modulus attack: Many reports[10-11] stated that the employ of a general composite modulus is risky. Certainly, if a message is transmitted to two entities that have relatively prime public keys, then the message can be decrypted. Since the text attack needs single message, the Lucas type scheme is susceptible to the general modulus attack. We will show this in the following assumption. Suppose (e_1,d_1) and (e_2,d_2) is the public and secret keys. Assume $m = r(M)$ is the message to be encrypted. Suppose e_1 and e_2 are co-prime, the attacker Oscar can decrypt m from the message $w_1 = r(W_1) \equiv r(e_1 * M) \bmod n$ and $w_2 = r(W_2) \equiv r(e_2 * M) \bmod n$ in the following way. Oscar applies the extended Euclidean method to obtain the integers j and a where $j * e_1 + a * e_2 = 1$. Then, Oscar finds $r(M) = r((j * e_1 + a * e_1)M) \equiv r(j * W_1 + a * W_2) \bmod n$. But if $r(j * W_1) \neq r(a * W_2) \bmod n$, then

$$m \equiv (w_1^3 + g * w_1 + t) * \left[\frac{\frac{y(j * W_1)}{y(W_1)} - \frac{y(e_2 * W_1)}{y(W_1)} * \frac{y(a * W_2)}{y(W_2)} * \left(\frac{y(e_1 * W_2)}{y(W_2)} \right)^{-1}}{r(j * W_1) - r(a * W_2)} \right]^2 - r(r * W_1) - r(a * W_2) \bmod n$$

Else

$$m \equiv \frac{\left[3 * r(j * W_1)^2 + g\right]^2}{4\left[r(j * W_1)^3 + g * r(j * W_1) + t\right]} - 2 * r(j * W_1) \bmod n$$

Proof: simple because

$y(e_2 * W_1) \equiv y(e_1 * W_2) \bmod n$.

CONCLUSION

We are introduced a different attack method on integer modulus. The new scheme has allowed raising an invulnerable message attack with a single message versus Lucas type scheme. This also verifies that the employ of asymmetric schemes is not really the best method to prevent the attacks.

REFERENCES

1. Rivest, R. L., A. Shamir and L. Adleman, 1978. A Method for Obtaining digital signatures and public key cryptosystems, Communications of the ACM, 2: 120-126
2. Denning, D. E., 1984. Digital Signatures with RSA and other public key cryptosystem, communications of the ACM, 27: 388-392.
3. Sattar Aboud, J., 2004. Baghdad Method for Calculating Multiplicative Inverse, International Conference on Information Technology, Las Vegas, Nevada, USA., pp: 816-819.
4. Sattar Aboud, J., 2005. Fraction - Integer Method (FIM) for Calculating Multiplicative Inverse, J. Systemics, Cybernetics and Informatics, Volume 2, Number 5, USA.

5. Miller, W. B. and R. Nobauer, 1981. Some remarks on public key cryptosystems, Science Math. Hunger, 16: 71-76.
6. Miller, W. B. and R. Nobauer, 1986. Cryptanalysis of the Dickson scheme, Advance in Cryptology - Euro-crypt 85, Lectures Notes in Comp. Sci., 219: 50-61
7. Bresoud, D.M., 1989. Factorization and primarily testing, Undergraduate Texts in Mathematics, Spring-Verlag
8. Smith, P.J and M.J.J. Lennon, 1993. A new public key system, Ninth IFIP Symposium on Computer Security pp: 103-117.
9. Bleichenbacher, D., W. Bosma and A.K. Lenstra, 1995. Some remarks on Lucas based cryptosystems, Advance in Cryptology, Crypto 95, volume 963 of Lectures Notes in Computer Science., pp: 386-396.
10. Sattar Aboud, J. and Mohammed Ahmed Al-Fayoumi, 2005 Two Efficient Digital and Multisignature Schemes, Proceeding of the IASTED International Conference on Computational Intelligence, Calgary, Canada, pp: 457-362.
11. Evon, M. Abu-Taieh and J. Sattar Aboud, 2003. A New Factoring Algorithm, International Conference on Security and Management SAM', 03, Las Vegas, Nevada USA. pp: 341-347