Enhancing the Massey-Omura Cryptosystem

Richard Winton, Ph.D. †

Abstract

The Massey-Omura Cryptosystem is a well known private key system. Although it is well designed and educational to study, the system has characteristics which make it vulnerable to cryptanalysis. In particular, the traditional Massey-Omura system is an exponential system which uses a prime modulus. Thus a cryptanalyst who is able to acquire the encryption key and modulus can easily calculate the corresponding decryption key and decipher intercepted messages. The systems developed in this paper follow the traditional Massey-Omura protocol, with two enhancements provided to improve security.

The enhanced Massey-Omura system (EMO-1) replaces the prime modulus with a composite which is the product of two distinct (large) primes. In this manner the system is provided with a level of security similar to that of an RSA public key system.

A stronger version of the enhanced Massey-Omura system (EMO-2) adds a digital signature to the EMO-1 system. The digital signature allows the recipient of a message encrypted with EMO-2 protocol to authenticate the identity of the sender, providing an additional aspect of security.

Introduction

Cryptosystems come in a wide variety of forms. One criteria for classifying cryptosystems is based on whether or not any of the encryption keys are made known to the public. Systems which make such information publicly known are referred to as "public key" cryptosystems. Others, which do not publish their encryption keys, are known as "private key" cryptosystems. This paper offers two generalizations of a known private key system called the Massey-Omura cryptosystem [1] whose mathematical basis is Fermat's Theorem.

The Massey-Omura Cryptosystem

The details of the Massey-Omura system construction as well as the correspondence protocol are described below.

Establishing the Communication System. In order to establish a Massey-Omura cryptosystem for a network of correspondents, the key center first performs the following functions.

1. An alphabet *A* is selected.
2. A maximum message length N is determined.
   Thus N is the maximum number of characters per message.

3. A scheme S is determined to convert alphabetic messages to numerical form and vice versa.
4. The largest integer L which can represent a message is determined based on the alphabet *A*, the maximum message length N, and the scheme S.
5. A prime p > L is selected as the network modulus.
6. For each member of the network, an integer w_i is selected as an encryption key such that $\gcd\{w_i, p-1\} = 1$.
7. For each integer w_i, $x_i = w_i^{-1}$ (mod p–1) is computed as a decryption key. The existence of x_i is guaranteed since w_i is an element of the group of units modulo p–1, while the computation of x_i is achieved using the Euclidean Algorithm.
8. Each network member is provided with their individual encryption and decryption keys w_i and x_i, respectively.
9. The parameters *A*, N, S, L, and p are published in the center directory. On the other hand, w_i and x_i are private keys, and are thus known only to the key center and the individual network member to whom they are assigned.

Correspondence Protocol. Suppose a network member Bob has keys $w_i = r$ and $x_i = t$, while network member Sue has keys $w_j = u$ and $x_j = v$. For Bob to send a message to Sue, the following protocol is observed.

1. Bob constructs his message m using the alphabet *A*, not to exceed the maximum message length N.
2. Bob converts his alphabetic message m to its numerical equivalent M ≤ L using the scheme S.
3. Bob enciphers M by computing M^r (mod p) and sends the result to Sue.
4. Sue further enciphers the transmission by computing $\left(M^r(\text{mod}\,p)\right)^u$ (mod p) = M^{ru} (mod p) and sends the result back to Bob.
5. Bob partially deciphers the transmission by computing $\left(M^{ru}(\text{mod}\,p)\right)^t$ (mod p) = $\left(M^u\right)^{rt}$ (mod p). Since t = r^{-1} (mod p–1), then rt ≡ 1(mod p–1), so that rt = 1 + s(p–1) for some integer s. Therefore $\left(M^u\right)^{rt}$ (mod p) = $\left(M^u\right)^{1+s(p-1)}$ (mod p) = $M^u \cdot \left(M^{p-1}\right)^{us}$ (mod p). However, since M ≤ L < p and p is prime, then gcd{M,p} = 1. Therefore $M^{p-1} \equiv 1$(mod p) by Fermat's Theorem. Hence $M^u \cdot \left(M^{p-1}\right)^{us}$ (mod p) ≡ M^u (mod p). Bob sends this result to Sue.
6. Sue completes the deciphering process by computing $\left(M^u(\text{mod}\,p)\right)^v$ (mod p) = M^{uv} (mod p) ≡ M (mod p) by the same

reasoning as in step 5 above since $v = u^{-1}$(mod p–1). Furthermore, M (mod p) = M since $M \leq L < p$.

7. Sue then converts M back to its alphabetic equivalent m using the scheme S and reads Bob’s message.

The correspondence protocol of the Massey-Omura Cryptosystem is illustrated in Figure I below.

Figure I

$$\begin{tikzcd}
\text{Bob }(r,t) \arrow[d] & \text{Sue }(u,v) \\
m \arrow[d] & \\
M \arrow[d] & \\
M^{r}\text{ (mod }p) \arrow[r] & M^{r}\text{ (mod }p) \arrow[d] \\
M^{ru}\text{ (mod }p) \arrow[d] & M^{ru}\text{ (mod }p) \arrow[l] \\
M^{rut}\text{ (mod }p)= M^{u}\text{ (mod }p) \arrow[r] & M^{u}\text{ (mod }p) \arrow[d] \\
 & M^{uv}\text{ (mod }p)=M \arrow[d] \\
 & m
\end{tikzcd}$$

The EMO-1 Cryptosystem

The EMO-1 cryptosystem, which is also a private key system, is an enhancement of the Massey-Omura cryptosystem. The basis for the EMO-1 cryptosystem is Euler's Theorem, which generalizes the result of Fermat's Theorem about prime moduli to include composite moduli as well. The enhancement is therefore achieved by replacing the prime modulus p of the Massey-Omura system with a positive integer n which is the product of two primes, thus improving the security of the system. The details of the system construction as well as the correspondence protocol are described below.

Establishing the Communication System. In order to establish an EMO-1 cryptosystem for a network of correspondents, the key center first performs the following functions.

1. An alphabet *A* is selected.
2. A maximum message length N is determined.
3. A scheme S is determined to convert alphabetic messages to numerical form and vice versa.
4. The largest integer L which can represent a message is determined based on the alphabet *A*, the maximum message length N, and the scheme S.
5. Distinct primes p > L and q > L are selected.
6. The network modulus n = pq as well as $\phi(n) = (p-1)(q-1)$ are computed.
7. For each member of the network, an integer w_i is selected as an encryption key such that $\gcd\{w_i, \phi(n)\} = 1$.
8. For each integer w_i, $x_i = w_i^{-1}$ (mod $\phi(n)$) is computed as a decryption key.
9. Each network member is provided with their individual encryption and decryption keys w_i and x_i, respectively.
10. The parameters *A*, N, S, L, and n are published in the center directory. On the other hand, w_i and x_i are private keys, and are thus known only to the key center and the individual network member to whom they are assigned.

Correspondence Protocol. Suppose a network member Bob has keys $w_i = r$ and $x_i = t$, while network member Sue has keys $w_j = u$ and $x_j = v$. For Bob to send a message to Sue, the following protocol is observed.

1. Bob constructs his message m using the alphabet *A*, not to exceed the maximum message length N.
2. Bob converts his alphabetic message m to its numerical equivalent $M \le L$ using the scheme S.
3. Bob enciphers M by computing M^r (mod n) and sends the result to Sue.
4. Sue further enciphers the transmission by computing $\left(M^r(\mathrm{mod}\, n)\right)^u$ (mod n) = M^{ru} (mod n) and sends the result back to Bob.
5. Bob partially deciphers the transmission by computing $\left(M^{ru}(\mathrm{mod}\, n)\right)^t$ (mod n) = $\left(M^u\right)^{rt}$ (mod n). Since $t = r^{-1}$ (mod $\phi(n)$), then $rt \equiv 1$(mod $\phi(n)$), so that $rt = 1 + s\cdot\phi(n)$ for some integer s. Therefore $\left(M^u\right)^{rt}$ (mod n) = $\left(M^u\right)^{1+s\cdot\phi(n)}$ (mod n) = $M^u \cdot \left(M^{\phi(n)}\right)^{us}$ (mod n). However, since $M \le L < p$, $M \le L < q$, p and q are primes, and n = pq, then gcd{M,n} = 1. Therefore $M^{\phi(n)} \equiv 1$(mod n) by Euler's Theorem. Hence $M^u \cdot \left(M^{\phi(n)}\right)^{us}$ (mod n) ≡ M^u (mod n). Bob sends this result to Sue.
6. Sue completes the deciphering process by computing

$\left(M^u (\bmod n)\right)^v$ (mod n) = M^{uv} (mod n) ≡ M (mod n) by the same reasoning as in step 5 above since v = u^{-1}(mod ϕ(n)). Furthermore, M (mod n) = M since M ≤ L < n.

7. Sue then converts M back to its alphabetic equivalent m using the scheme S and reads Bob’s message.

The correspondence protocol of the EMO-1 Cryptosystem is illustrated in Figure II below.

Figure II

$$\begin{tikzcd}
\text{Bob } (r,t) \arrow[d] & \text{Sue } (u,v) \\
m \arrow[d] & \\
M \arrow[d] & \\
M^r \text{ (mod n)} \arrow[r] & M^r \text{ (mod n)} \arrow[d] \\
M^{ru} \text{ (mod n)} \arrow[d] & M^{ru} \text{ (mod n)} \arrow[l] \\
M^{rut} \text{ (mod n)} = M^u \text{ (mod n)} \arrow[r] & M^u \text{ (mod n)} \arrow[d] \\
 & M^{uv} \text{ (mod n)} = M \arrow[d] \\
 & m
\end{tikzcd}$$

Observations. Since the prime system modulus p is published in the Massey-Omura system, then ϕ(p) = p–1 is readily known to the public. Thus if a network member's private encryption key w_i is discovered by an interceptor, then the interceptor can easily compute the network member's corresponding key x_i = w_i^{-1}(mod p–1) for decryption purposes in the same manner as done by the key center using the Euclidean Algorithm.

However, in the EMO-1 cryptosystem, note that only the key center has knowledge of p and q. Therefore, even though n is published, it is difficult for others to factor n = pq, and thus to compute ϕ(n) = (p–1)(q–1), for sufficiently large n. Consequently, even if a network member's private encryption key w_i is discovered by an unauthorized person, that person cannot use w_i compute the network member's corresponding key $x_i = w_i^{-1} (\text{mod } \phi(n))$ for decryption purposes. This constitutes an improvement in security over the Massey-Omura cryptosystem.

The EMO-2 Cryptosystem

The EMO-2 cryptosystem is an enhancement of the EMO-1 cryptosystem described above. The enhancement is achieved by adding a second layer of encryption to each transmission, making cryptanalysis more difficult for those who would intercept the message without authorization. Furthermore, the system employs a digital signature [4] which enables the recipient of a message to verify the identity of the sender, providing still another dimension of security. The result is a partially private key, partially public key cryptosystem. More specifically, the EMO-2 cryptosystem is a combination of an EMO-1 private key system and an RSA public key system [2,3]. The details of the system construction as well as the correspondence protocol are described below.

Establishing the Communication System. In order to establish an EMO-2 cryptosystem for a network of correspondents, the key center first performs the following functions.

1. An alphabet *A* is selected.
2. A maximum message length N is determined.
3. A scheme S is determined to convert alphabetic messages to numerical form and vice versa.
4. The largest integer L which can represent a message is determined based on the alphabet *A*, the maximum message length N, and the scheme S.
5. Distinct primes p > L and q > L are selected.
6. The network modulus n = pq as well as $\phi(n) = (p-1)(q-1)$ are computed.
7. For each member of the network, an integer w_i is selected as a primary encryption key such that $\gcd\{w_i, \phi(n)\} = 1$.
8. For each integer w_i, $x_i = w_i^{-1} (\text{mod } \phi(n))$ is computed as a primary decryption key.
9. For each member of the network, an integer y_i is selected as a secondary encryption key such that $y_i \neq w_i$, $y_i \neq x_i$, and $\gcd\{y_i, \phi(n)\} = 1$.
10. For each integer y_i, $z_i = y_i^{-1} (\text{mod } \phi(n))$ is computed as a secondary decryption key.
11. Each network member is provided with their individual encryption and decryption keys w_i, x_i, y_i, and z_i.
12. The keys $\{y_i\}$, along with the parameters *A*, N, S, L, and n, are published in the center directory. On the other hand, w_i, x_i, and z_i are private keys, and are thus known only to the key center and the individual network member to whom they are assigned.

Correspondence Protocol. Suppose a network member Bob has keys $w_i = r$, $x_i = t$, $y_i = c$, and $z_i = b$, while network member Sue has keys $w_j = u$, $x_j = v$, $y_j = e$, and $z_j = d$. For Bob to send a message to Sue, the following protocol is observed.

1. Bob constructs his message m using the alphabet *A*, not to exceed the maximum message length N.
2. Bob converts his alphabetic message m to its numerical equivalent $M \le L$ using the scheme S.
3. Bob enciphers M by computing $M^r \pmod n$.
4. Bob further enciphers M by computing $\left(M^r (\operatorname{mod} n)\right)^e \pmod n = M^{re} \pmod n$ and sends the result to Sue.
5. Sue partially deciphers the transmission by computing $\left(M^{re} (\operatorname{mod} n)\right)^d \pmod n = \left(M^r\right)^{ed} \pmod n = M^r \pmod n$ by Euler's Theorem as in the EMO-1 cryptosystem since $d = e^{-1} (\operatorname{mod} \phi(n))$.
6. Sue further enciphers the transmission by computing $\left(M^r (\operatorname{mod} n)\right)^u \pmod n = M^{ru} \pmod n$ and sends the result back to Bob.
7. Bob partially deciphers the transmission by computing $\left(M^{ru} (\operatorname{mod} n)\right)^t \pmod n = \left(M^u\right)^{rt} \pmod n = M^u \pmod n$ by the same reasoning as in step 5 above since $t = r^{-1} (\operatorname{mod} \phi(n))$.
8. Bob then adds a layer of encryption back by computing $\left(M^u (\operatorname{mod} n)\right)^e \pmod n = M^{ue} \pmod n$.
9. Bob now places the digital signature on the message by computing $\left(M^{ue} (\operatorname{mod} n)\right)^b \pmod n = M^{ueb} \pmod n$ and sends the result to Sue.
10. Sue partially deciphers the transmission by computing $\left(M^{ueb} (\operatorname{mod} n)\right)^c \pmod n = \left(M^{ue}\right)^{bc} \pmod n \equiv M^{ue} \pmod n$ by the same reasoning as in step 5 above since $c = b^{-1} (\operatorname{mod} \phi(n))$.
11. Sue continues deciphering the transmission by computing $\left(M^{ue} (\operatorname{mod} n)\right)^d \pmod n = \left(M^u\right)^{ed} \pmod n \equiv M^u \pmod n$ by the same reasoning as in step 5 above since $d = e^{-1} (\operatorname{mod} \phi(n))$.
12. Sue completes the deciphering process by computing $\left(M^u (\operatorname{mod} n)\right)^v \pmod n = M^{uv} \pmod n \equiv M \pmod n$ by the same reasoning as in step 5 above since $v = u^{-1} (\operatorname{mod} \phi(n))$. Furthermore, $M \pmod n = M$ since $M \le L < n$.
13. Sue then converts M back to its alphabetic equivalent m using the scheme S and reads Bob's message.

The correspondence protocol of the EMO-2 cryptosystem is illustrated in Figure III below.

Figure III

$$\begin{tikzcd}
\text{Bob } (r,t,c,b) \arrow[d] & \text{Sue } (u,v,e,d) \\
m \arrow[d] & \\
M \arrow[d] & \\
M^{r} \text{ (mod n)} \arrow[d] & \\
M^{re} \text{ (mod n)} \arrow[r] & M^{re} \text{ (mod n)} \arrow[d] \\
& M^{red} \text{ (mod n)} = M^{r} \text{ (mod n)} \arrow[d] \\
M^{ru} \text{ (mod n)} \arrow[d] & M^{ru} \text{ (mod n)} \arrow[l] \\
M^{rut} \text{ (mod n)} = M^{u} \text{ (mod n)} \arrow[d] & \\
M^{ue} \text{ (mod n)} \arrow[d] & \\
M^{ueb} \text{ (mod n)} \arrow[r] & M^{ueb} \text{ (mod n)} \arrow[d] \\
& M^{uebc} \text{ (mod n)} = M^{ue} \text{ (mod n)} \arrow[d] \\
& M^{ued} \text{ (mod n)} = M^{u} \text{ (mod n)} \arrow[d] \\
& M^{uv} \text{ (mod n)} = M \arrow[d] \\
& m
\end{tikzcd}$$

More Observations. It is important to note that, while the sender and receiver each have two pairs of encryption and decryption keys, they are used quite differently. The primary keys assigned initially (r ant t for Bob; u and v for Sue) are used with the Massey-Omura protocol. However, the secondary keys assigned (c and b for Bob; e and d for Sue) are used with the RSA protocol.

Similar to the EMO-1 cryptosystem, only the key center has knowledge of p and q. Therefore, even though n is published, it is difficult for others to factor n = pq, and thus to compute $\phi(n) = (p-1)(q-1)$, for sufficiently large n. Consequently, even if a network member's private encryption key w_i is discovered by an interceptor, the interceptor cannot compute the network member's corresponding key $x_i = w_i^{-1} \pmod{\phi(n)}$ for decryption purposes. In fact, even with y_i published, the corresponding key $z_i = y_i^{-1} \pmod{\phi(n)}$ cannot be computed by an interceptor.

However, as mentioned above, a primary security improvement of the EMO-2 cryptosystem over the EMO-1 cryptosystem is the double encryption provided with each transmission to make cryptanalysis by interceptors more difficult. It is noteworthy that the exponentiation performed in step 9 does not represent a triple encryption. Since $c = b^{-1} \pmod{\phi(n)}$ is published, it would be relatively simple for an interceptor who understood the system being used to remove b by applying the key c. Thus the exponentiation by b provides no real additional encryption. Instead, the exponent b serves as the digital signature by which Sue can verify Bob's identity as the sender. For if Sue applies Bob's public encryption key c and the results (after the rest of the deciphering process) yield readable text, then the message must have been encrypted by the sender with the exponent b. However, b is Bob's private decryption key, which is known only to Bob and the key center. Therefore, unless the key center is playing a trick on Sue, the message must have come from Bob.

† *Richard Winton, Ph.D.*, Tarleton State University, Stephenville, TX, USA

References

[1] Lewand, R. E., “Cryptological Mathematics”, *The Mathematical Association of America*, Washington DC, 2000.

[2] Rivest R. L., Shamir A., and Adleman L. M. , “A method for obtaining digital signatures and public-key cryptosystems”, *Communications of the ACM*, Volume 21 (1978), 120-126.

[3] Rivest R. L., Shamir A., and Adleman L. M., “Cryptographic communications system and method”, United States Patent #4,405,8239, issued September 20, 1983.

[4] K. H. Rosen, “Elementary Number Theory”, 4th ed., *Addison Wesley Longman*, New York, 2000.