Combining Public and Private Key Cryptography

Richard Winton, Ph.D. †

Abstract

Cryptosystems may be classified as either public or private key. The system developed in this paper combines the protocols of these two types of cryptography to produce a three-pass system that is more secure than with either one alone. Each transmission in the correspondence protocol is at least doubly encrypted. Furthermore, a digital signature is employed. Finally, recent advances in number theory provide a greater computational efficiency than exists in similar previously established systems.

Introduction

In 1978 Ronald Rivest, Adi Shamir, and Leonard Aldeman produced the RSA public key cryptosystem ([9],[10]) based on Euler's Theorem. The first private key, three-pass system was developed by Adi Shamir around 1980 ([4, p. 345],[7, p. 535]). Also known as Shamir's no-key protocol [7, p. 535], this system requires three transmissions to complete the transfer of information to the recipient in a form that can be successfully deciphered [7, p. 500, no. 12.22]. In 1982 James L. Massey and Jim K. Omura produced the Massey-Omura private key cryptosystem ([5, p. 174],[6]) whose mathematical basis is Fermat's Theorem. Thought to be an improvement over the Shamir three-pass system, the Massey-Omura Cryptosystem is a private key, three-pass, exponential system which uses a prime modulus. By the late 1980's these three-pass systems were eventually developed into three-pass, zero-knowledge protocol systems ([2],[3],[8, pp. 255-256]). In 2007 Richard A. Winton [12] developed two cryptosystems which improved the security of the Massey-Omura system.

The Enhanced Massey-Omura 1 (EMO-1) Cryptosystem [12] is a private key, three-pass system which replaced the prime modulus of the Massey-Omura system ([5, p. 174],[6]) with a composite modulus to increase the difficulty of cryptanalysis. Also a three-pass system, the Enhanced Massey-Omura 2 (EMO-2) Cryptosystem [12] combined the private key protocols of the Massey-Omura and EMO-1 systems with the public key protocol of the RSA system. As a result, EMO-2 protocol increased the security of the Massey-Omura and EMO-1 systems by providing double encryption on each transmission, as well as a digital signature [11, p. 300] which enables the recipient of an encrypted transmission to authenticate the identity of the sender.

The Winton Cryptosystem

Similar to the EMO-2 Cryptosystem [12], the Winton Cryptosystem is a partially private key, partially public key three-pass system which combines the methods of the EMO-1 and RSA systems. Furthermore, its correspondence

protocol is based primarily on that of the EMO-2 Cryptosystem. However, the Winton Cryptosystem contains characteristics which make it both more secure and more efficient than the EMO-2 system.

Although each transmission in the EMO-2 Cryptosystem [12] is doubly encrypted, the security of the transmissions does present a small risk in the fact that the key center knows all of the cryptological parameters and keys of the system. Thus an unscrupulous employee at the key center could read the messages of the network members, or could even sell knowledge of these keys to others. The Winton Cryptosystem addresses this vulnerability by ensuring that each of the transmissions in the three-pass correspondence protocol is secured with a cryptological lock to which only the recipient holds the key. Furthermore, even though the key center has the keys with which each transmission is encrypted, the decryption key not known to the key center in each transmission cannot be calculated with the parameters known to the key center. In this manner the multiple encryption and digital signature provided by the EMO-2 system are maintained, but the key center is unable to decipher any of the transmissions in the three-pass protocol.

Finally, the encryption and decryption processes of both the EMO-1 and EMO-2 Cryptosystems [12] are based on Euler's Theorem. Consequently these systems have a somewhat limited computational efficiency. However, Richard A. Winton established results in 2009 [13] which allow the Winton Cryptosystem to operate with a greater computational efficiency than the EMO-1 and EMO-2 systems.

The sources of the improvements discussed above will be revealed shortly. First, however, the details of the system structure and correspondence protocol of the Winton Cryptosystem must be presented.

System Structure

In order to construct a Winton 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 of N alphabet characters is determined.
3. A scheme S is determined to convert alphabetic messages to unique positive integers in a one-to-one correspondence 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 and q are selected such that $pq > L$.
6. The network modulus $n = pq > L$ and $\phi(n) = (p-1)(q-1)$ are computed.
7. For each network member, a least residue w_i modulo $\phi(n)$ is selected as a primary encryption key such that $\gcd\{w_i, \phi(n)\} = 1$.
8. For each primary encryption key w_i, $x_i = w_i^{-1} \pmod{\phi(n)}$ is computed as a primary decryption key.
9. Each network member is provided with their individual primary 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 network member to whom they are assigned.

After the functions above are performed by the key center, each network member individually performs the following functions.

11. Each member selects distinct primes p_i and q_i such that $p_i q_i > n$.
12. Each member computes their own personal modulus $n_i = p_i q_i > n$ and $\phi(n_i) = (p_i - 1)(q_i - 1)$.
13. Each member selects a least residue y_i modulo $\phi(n_i)$ as a secondary encryption key such that $y_i \neq w_i$, $y_i \neq x_i$, and $\gcd\{y_i, \phi(n_i)\} = 1$.
14. Each member computes $z_i = y_i^{-1} \pmod{\phi(n_i)}$ as a secondary decryption key.
15. Each member publishes their encryption key y_i and modulus n_i in the key center directory, keeping the decryption key z_i private.

Thus the parameters published in the key center directory include *A*, N, S, L, n, $\{n_i\}$, and $\{y_i\}$. Furthermore, the key center knows p, q, $\phi(n)$, $\{w_i\}$, and $\{x_i\}$. Each network member also knows their individual private keys w_i, x_i, and z_i, as well as the parameters p_i, q_i, and $\phi(n_i)$. It is important to note that the key center does not know any of $\{z_i\}$, $\{p_i\}$, $\{q_i\}$, and $\{\phi(n_i)\}$.

Correspondence Protocol

Suppose that Bob and Sue are members of a Winton Cryptosystem network with system modulus n. Suppose also that Bob has personal modulus $n_i = h$ and keys $w_i = r$, $x_i = t$, $y_i = c$, and $z_i = b$, while Sue has personal modulus $n_j = k$ and 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 $M \leq L$ using the scheme S.
3. Bob enciphers M by computing $M^r \pmod{n}$.
4. Bob further enciphers M by computing $\left(M^r \pmod{n}\right)^e \pmod{k}$ and sends the result to Sue.
5. Sue partially deciphers the transmission by computing

$\left[\left(M^r \pmod n\right)^e \pmod k\right]^d \pmod k = \left(M^r \pmod n\right)^{ed} \pmod k = M^r \pmod n.$

Since $M^r \pmod n < n < k$, then $k \nmid M^r \pmod n$. Therefore $\left(M^r \pmod n\right)^{ed} \pmod k = \left(M^r \pmod n\right) \pmod k$ since $d = e^{-1} \pmod{\phi(k)}$ [13, Corollary 10]. Furthermore, $\left(M^r \pmod n\right) \pmod k = M^r \pmod n$ since $M^r \pmod n < n < k$.

6. Sue adds encryption by computing $\left(M^r \pmod n\right)^u \pmod n = M^{ru} \pmod n$.
7. Sue adds more encryption by computing $\left(M^{ru} \pmod n\right)^c \pmod h$ and sends the result back to Bob.
8. Bob partially deciphers the transmission by computing $\left[\left(M^{ru} \pmod n\right)^c \pmod h\right]^b \pmod h = \left(M^{ru} \pmod n\right)^{cb} \pmod h = M^{ru} \pmod n$.

   Since $M^{ru} \pmod n < n < h$, then $h \nmid M^{ru} \pmod n$. Therefore $\left(M^{ru} \pmod n\right)^{cb} \pmod h = \left(M^{ru} \pmod n\right) \pmod h$ since $b = c^{-1} \pmod{\phi(h)}$ [13, Corollary 10]. Furthermore, $\left(M^{ru} \pmod n\right) \pmod h = M^{ru} \pmod n$ since $M^{ru} \pmod n < n < h$.
9. Bob further deciphers the transmission by computing $\left(M^{ru} \pmod n\right)^t \pmod n = \left(M^u\right)^{rt} \pmod n = M^u \pmod n$.

   Since $M \le L < n$, then $n \nmid M$. Therefore either $p \nmid M$ or $q \nmid M$ since $n = pq$ and $p \ne q$. Thus either $p \nmid M^u$ or $q \nmid M^u$, and so $n \nmid M^u$. Hence $\left(M^u\right)^{rt} \pmod n = M^u \pmod n$ since $t = r^{-1} \pmod{\phi(n)}$ [13, Corollary 10].

Case 1: $h \le k$

10. Bob adds the digital signature by computing $\left(M^u \pmod n\right)^b \pmod h$.
11. Bob adds a layer of encryption by computing $\left[\left(M^u \pmod n\right)^b \pmod h\right]^e \pmod k$ and sends the result to Sue.
12. Sue partially deciphers the transmission by computing

    $\left[\left[\left(M^u \pmod n\right)^b \pmod h\right]^e \pmod k\right]^d \pmod k =$

    $\left[\left(M^u \pmod n\right)^b \pmod h\right]^{ed} \pmod k = \left(M^u \pmod n\right)^b \pmod h$

    as in step 5 since $d = e^{-1} \pmod{\phi(k)}$ [13, Corollary 10] and $\left(M^u \pmod n\right)^b \pmod h < h \le k$.
13. Sue continues deciphering the transmission by computing $\left[\left(M^u \pmod n\right)^b \pmod h\right]^c \pmod h = \left(M^u \pmod n\right)^{bc} \pmod h = M^u \pmod n$

as in step 8 since $c = b^{-1} \pmod{\phi(h)}$ [13, Corollary 10] and $M^u \pmod{n} < n < h$.

Case 2: $h > k$

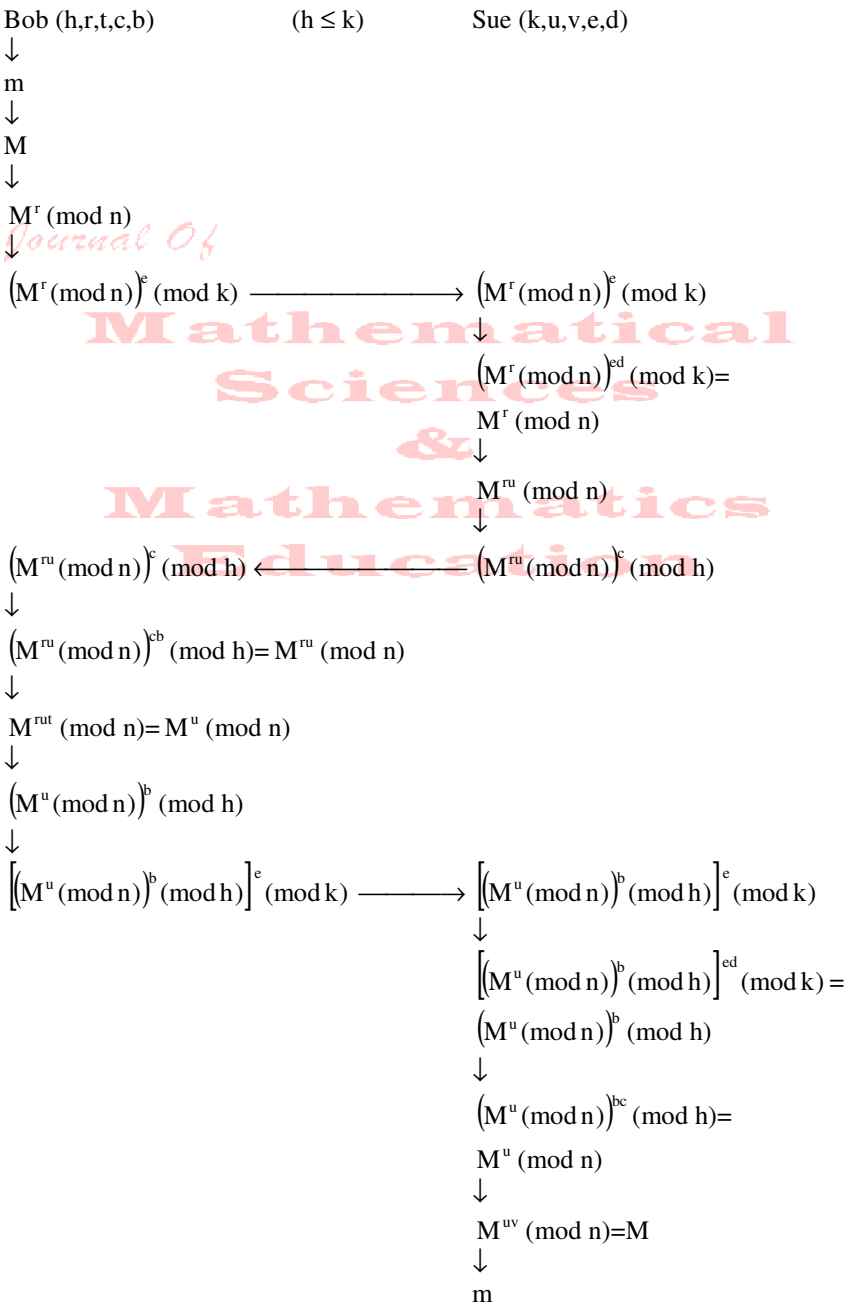
10. Bob adds a layer of encryption by computing $\left(M^u \pmod{n}\right)^e \pmod{k}$.
11. Bob adds the digital signature by computing $\left[\left(M^u \pmod{n}\right)^e \pmod{k}\right]^b \pmod{h}$ and sends the result to Sue.
12. Sue partially deciphers the transmission by computing $\left[\left[\left(M^u \pmod{n}\right)^e \pmod{k}\right]^b \pmod{h}\right]^c \pmod{h} =$ $\left[\left(M^u \pmod{n}\right)^e \pmod{k}\right]^{bc} \pmod{h} = \left(M^u \pmod{n}\right)^e \pmod{k}$ as in step 8 since $c = b^{-1} \pmod{\phi(h)}$ [13, Corollary 10] and $\left(M^u \pmod{n}\right)^e \pmod{k} < k < h$.
13. Sue continues deciphering the transmission by computing $\left[\left(M^u \pmod{n}\right)^e \pmod{k}\right]^d \pmod{k} = \left(M^u \pmod{n}\right)^{ed} \pmod{k} = M^u \pmod{n}$ as in step 5 since $d = e^{-1} \pmod{\phi(k)}$ [13, Corollary 10] and $M^u \pmod{n} < n < k$.

Protocol Completion

14. In either case, Sue completes the deciphering process by computing $\left(M^u \pmod{n}\right)^v \pmod{n} = M^{uv} \pmod{n} = M \pmod{n}$ as in step 9 since $v = u^{-1} \pmod{\phi(n)}$ [13, Corollary 10]. Furthermore, $M \pmod{n} = M$ since $M \le L < n$.
15. Sue then converts M to its alphabetic equivalent m using the scheme S and reads Bob's message.

The correspondence protocol of the Winton Cryptosystem is illustrated in Figure 1 below. Figure 1 corresponds to Case 1 in which $h \le k$. A similar flowchart can easily be constructed for Case 2 in which $h > k$.

Figure 1



Observations

The primary and secondary decryption keys x_i and z_i are calculated in steps 8 and 14 of the system structure, respectively. Note that in step 7 w_i is selected such that $\gcd\{w_i, \phi(n)\} = 1$. Therefore w_i is an element of the group of units modulo $\phi(n)$ [1, p. 97, Example 3.1.4]. Consequently the existence and uniqueness of $x_i = w_i^{-1} \pmod{\phi(n)}$ is guaranteed [11, p. 139, Theorem 4.10]. A similar argument exists for $z_i = y_i^{-1} \pmod{\phi(n_i)}$. Furthermore, the computation of the decryption keys x_i and z_i can be achieved by using an extended version of the Euclidean Algorithm [11, p. 141, Example 4.15]. In fact, the same process verifies the existence of these keys before the computation is complete.

In steps 10 and 11, the sender Bob must choose in which order to apply the exponents b and e based upon whether $h \leq k$ or $h > k$. (Actually, if $h = k$ then the order in which b and e are applied is irrelevant. However, the key center would not allow a situation in which $h = k$.) Note that the information necessary for making such a decision is available to Bob (and Sue as well) since the moduli h and k are published in the key center directory. In fact, the sender and recipient are each required to use both h and k in the three-pass correspondence protocol.

Similar to the EMO-2 Cryptosystem [12], the Winton Cryptosystem provides at least double encryption with each transmission in the three-pass protocol to make cryptanalysis by interceptors more difficult. It is noteworthy that triple encryption is provided in step 7 before Sue transmits to Bob. However, the exponentiations performed in steps 10 and 11 do not actually produce another triple encryption. Since h and $c = b^{-1} \pmod{\phi(h)}$ are published, it would be relatively simple for an interceptor who understood the system structure and protocol to remove the exponent b by applying the key c modulo h. 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 [11, p. 300]. 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 previously encrypted by the sender with the exponent b. However, b is Bob's private decryption key, which is known only to Bob. Consequently Bob must have sent the message. Hence Sue is able to authenticate Bob's identity as the sender.

Also similar to the EMO-2 Cryptosystem [12], the primary keys assigned initially (r ant t for Bob; u and v for Sue) are used with the Massey-Omura protocol ([5, p. 175],[6]). However, the secondary keys assigned (c and b for Bob; e and d for Sue) are used with the RSA protocol ([5, p. 152],[9],[10]).

Each of the primary encryption keys ($w_i = r$ and $w_j = u$) used in each transmission has a corresponding decryption key known only to the key center and either the sender or recipient. Similar to the EMO-1 and EMO-2 systems

[12], only the key center has knowledge of p and q. Therefore, even though n is published, it is difficult 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 primary encryption key, say w_j, is discovered by an interceptor, the interceptor cannot compute the network member's corresponding key $x_j = w_j^{-1} \pmod{\phi(n)}$ for decryption purposes. The key center, however, knows the keys $\{x_i\}$, and can thus remove an encryption produced with the key w_j.

In contrast, each of the secondary encryption keys ($y_i = c$ and $y_j = e$) used in each transmission of the three-pass protocol has a corresponding decryption key known only to the recipient of that specific transmission. Furthermore, p_i and q_i are known only to the network member who selects them. Thus even though n_i is published, it is difficult for anyone else to factor $n_i = p_i q_i$, and thus to compute $\phi(n_i) = (p_i - 1)(q_i - 1)$, for sufficiently large n_i. Consequently, even with n_i and y_i being published, $z_i = y_i^{-1} \pmod{\phi(n_i)}$ cannot be computed for decryption purposes by anyone other than the network member to whom z_i is assigned. Hence none of the three transmissions can be deciphered by an interceptor, including the key center itself. This is the particular feature of the Winton Cryptosystem which addresses the weakness of the EMO-2 Cryptosystem security discussed above by making transmissions secure from cryptanalysis even by the key center.

Note that the multiple encryption and digital signature of the Winton Cryptosystem protocol is accomplished by successive exponentiations relative to different moduli. Furthermore, although $\left[a^r \pmod n\right]^t \pmod n \equiv a^{rt} \pmod n$, in general we have $\left[a^r \pmod{n_1}\right]^t \pmod{n_2} \not\equiv \left[a^t \pmod{n_2}\right]^r \pmod{n_1}$. This potential problem with the decryption process is avoided by encrypting with sequential exponentiations in order of increasing corresponding moduli.

Finally, since decryption in the EMO-1 and EMO-2 Cryptosystems are based on Euler's Theorem, then the prime factors p and q of the modulus n in those systems are selected so that if L is the largest possible numerical equivalent of a message, then p > L and q > L [12]. These conditions for p and q are necessary to guarantee that the numerical representation of any message is relatively prime with the modulus for the application of Euler's Theorem during decryption. Consequently $n = pq > L^2$, requiring a relatively large modulus n. However, decryption in the Winton Cryptosystem uses results established in 2009 by Richard A. Winton [13] rather than Euler's Theorem. More specifically, the selection of p and q for the primary modulus n require only that n = pq > L ([13, Theorem 8],[13, Corollary 10]). Hence the primary modulus n of the Winton Cryptosystem is on the order of the square root of the moduli of the EMO-1 and EMO-2 Cryptosystems. Furthermore, the same principle is applied to the selection of the primes $\{p_i\}$ and $\{q_i\}$ for the individual secondary moduli

$\{n_i\}$. These smaller moduli allow the Winton Cryptosystem to operate with a greater computational efficiency than the EMO-1 and EMO-2 systems.

Concluding Remarks

The results of Winton ([13, Theorem 8],[13, Corollary 10]) which improve the computational efficiency of the Winton Cryptosystem through the use of smaller moduli can also be applied in the same manner to enhance the efficiency of the EMO-1 and EMO-2 Cryptosystems [12]. However, unlike the Winton Cryptosystem, the key center would still have the ability to decipher transmissions encrypted by EMO-1 or EMO-2 protocol.

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

References

1. J. A. Beachy and W. D. Blair, *Abstract Algebra with a Concrete Introduction*, Prentice Hall, Englewood Cliffs, New Jersey, 1990.
2. U. Feige, A. Fiat, and A. Shamir, *Zero-knowledge Proofs of Idenity*, Proceedings of the 19th Annual ACM Symposium on the Theory of Computing, (1987) pp. 210-217.
3. U. Feige, A. Fiat, and A. Shamir, *Zero-knowledge Proofs of Idenity*, Journal Cryptology, Vol. 1, No. 2, (1988) pp. 77-94.
4. A. G. Konheim, *Cryptography, A Primer*, John Wiley & Sons, New York, 1981.
5. R. E. Lewand, *Cryptological Mathematics*, The Mathematical Association of America, Washington DC, 2000.
6. J. L. Massey and J. K. Omura, *Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission*, United States Patent #4,567,600, issued January 28, 1986.
7. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Inc., New York, 1997.
8. R. A. Mollin, *An Introduction to Cryptography*, Chapman & Hall/CRC, New York, 2001.
9. R. L. Rivest, A. Shamir, and L. M. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, Volume 21 (1978), pp. 120-126.
10. R. L. Rivest, A. Shamir, and L. M. Adleman, *Cryptographic communications system and method*, United States Patent #4,405,8239, issued September 20, 1983.
11. K. H. Rosen, *Elementary Number Theory*, 4th edition, Addison-Wesley, New York, 2000.
12. R. A. Winton, *Enhancing the Massey-Omura Cryptosystem*, Journal of Mathematical Sciences and Mathematics Education, Vol. 2, No. 1, (2007) pp. 21-29.
13. R. A. Winton, *Modular Exponentiations and the Identity Map on* $\mathbf{Z}_n$,

Journal of Mathematical Sciences and Mathematics Education, Vol. 4, No. 2, (2009) pp. 1-6.