A Polygraphic, Polyalphabetic Cryptosystem with Public Key and Private Key Encryption

Richard Winton, Ph.D. †
Jeremiah Bass, Ph.D. ‡

Abstract

Cryptosystems may be classified as either public key or private key. The system developed in this paper combines the protocols of these two types of cryptography. Techniques and characteristics of previously established cryptosystems are employed as well to produce a three-pass system that is more secure than these earlier systems. Each transmission in the correspondence protocol is at least triply encrypted. The system is also both polygraphic and polyalphabetic in nature. Furthermore, a digital signature enhances the system security by enabling the recipient of an encrypted message to authenticate the identity of the sender. Finally, a greater computational efficiency is achieved than exists in similar previously established systems due to recent results in number theory.

Introduction

In 1978 Ronald Rivest, Adi Shamir, and Leonard Aldeman produced the RSA public key cryptosystem [9] based on Euler's Theorem. This system was later patented in 1983 [10]. The first private key three-pass system was developed by Adi Shamir around 1980 [4, p. 345]. 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 three-pass private key cryptosystem [5, p. 174], whose mathematical basis is Fermat's Theorem, and which was patented in 1986 [6]. Considered to be an improvement of 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 such three-pass systems were eventually developed into three-pass, zero-knowledge protocol systems ([2],[3],[8, pp. 255-256]).

In 2007 Richard A. Winton developed two cryptosystems [12] which resemble the Massey-Omura system ([5, p. 174],[6]) but are more secure. Specifically, the Enhanced Massey-Omura 1 (EMO-1) Cryptosystem [12] is a private key three-pass system which replaces the prime modulus of the Massey-Omura system with a composite modulus to increase the difficulty of cryptanalysis. Also a three-pass system, the Enhanced Massey-Omura 2 (EMO-2) Cryptosystem [12] combines the private key protocol of the Massey-Omura system and the composite modulus of the EMO-1 system with the public key protocol of the RSA system. As a result, the EMO-2 protocol increases 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.

Similar to the EMO-2 Cryptosystem [12], the Winton Cryptosystem [14] published in 2012 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 is vulnerable due to the fact that the key center knows all of the cryptological parameters and keys of the system. Consequently there is a risk that an 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 [14] 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 of that specific transmission 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 by the Winton Cryptosystem, 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 due to the size of the prime factors of the system moduli. However, results in number theory established in 2009 by Richard A. Winton [13] enable the Winton Cryptosystem [14] to operate with a greater computational efficiency than the EMO-1 and EMO-2 systems by reducing the sizes of the prime factors of the system moduli to approximately the square roots of their sizes in both the EMO-1 and EMO-2 systems.

The Winton-Bass Cryptosystem

Similar to the EMO-2 Cryptosystem [12] and Winton Cryptosystem [14], the Winton-Bass Cryptosystem presented here is a three-pass system which uses both private key and public key cryptography by combining the methods of the EMO-1 [12] and RSA [5, pp. 150-160] systems. Furthermore, the Winton-Bass correspondence protocol is based primarily on that of the EMO-2 and Winton Cryptosystems. Like the Winton Cryptosystem, the Winton-Bass system attaches a cryptological lock to each of the transmissions in the three-pass protocol for which only the recipient of that particular transmission holds the decryption key, so that even key center personnel cannot decipher intercepted messages. The digital signature of the EMO-2 and Winton systems which enables the recipient of a message to authenticate the identity of the sender is also retained in the Winton-Bass system. Finally, the number theoretic results ([13, Theorem 8],[13, Corollary 10]) employed by the Winton system to improve the computational efficiency of the EMO-2 system are incorporated into the Winton-Bass system.

However, the Winton-Bass Cryptosystem contains characteristics which make it more secure than the EMO-1, EMO-2, and Winton systems. While the EMO-2 and Winton systems provide at least double encryption in each transmission of the three-pass protocol, each transmission of the Winton-Bass system is at least triply encrypted for enhanced security. Furthermore, the Winton-Bass Cryptosystem also uses matrix encryption and decryption, resulting in a system which is polygraphic [5, p. 103]. Finally, the matrix encryption simultaneously produces a system which is polyalphabetic, a characteristic which is desirable since it disguises the natural frequencies of the alphabet characters [5, p. 45].

The mathematical details of the characteristics of the Winton-Bass Cryptosystem discussed above will be explained later. First, however, the system structure and correspondence protocol are presented.

System Structure

In order to construct a Winton-Bass Cryptosystem for a network of correspondents, the key center first performs the following functions.

1. An alphabet *A* is selected.
2. A size α for a square matrix is selected, where α is an integer and $\alpha > 1$.
3. A maximum string length of β alphabet characters is determined. Thus the maximum message length per transmission is $\alpha\beta$ characters.
4. A scheme S is determined to convert alphabetic strings of length β to unique positive integers in a one-to-one correspondence and vice versa.
5. The largest integer L which can represent a character string is determined based on the alphabet *A*, the maximum string length β, and the scheme S.
6. Distinct primes p and q are selected such that $pq > L$.
7. The network modulus $n = pq > L$ and $\phi(n) = (p-1)(q-1)$ are computed.
8. An $\alpha \times \alpha$ nonsingular, diagonal system encryption matrix Q is constructed so that the diagonal entries $\{Q_{ii}\}_{i=1}^{\alpha}$ of Q are distinct (nonzero) least residues modulo n which are relatively prime to n.
9. For each network member, a least residue w_i modulo $\phi(n)$ is selected as a primary encryption key such that $\gcd\{w_i, \phi(n)\} = 1$.
10. For each primary encryption key w_i, $x_i = w_i^{-1} \pmod{\phi(n)}$ is computed as a primary decryption key.
11. Each network member is provided with their individual primary encryption and decryption keys w_i and x_i, respectively.

12. Parameters *A*, Q, S, L, α, β, 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.

13. Each member selects distinct primes p_i and q_i such that $p_i q_i > n$.
14. Each member computes their own personal modulus $n_i = p_i q_i > n$ and $\phi(n_i) = (p_i - 1)(q_i - 1)$.
15. 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 $\gcd\{y_i, \phi(n_i)\} = 1$.
16. Each member computes $z_i = y_i^{-1}$ (mod $\phi(n_i)$) as a secondary decryption key.
17. 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*, Q, S, L, α, β, n, $\{n_i\}$, and $\{y_i\}$. Furthermore, the key center knows p, q, ϕ(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 $\{\phi(n_i)\}$. Since the moduli $\{n_i\}$ are sufficiently large, then the key center cannot factor $n_i = p_i q_i$ to obtain $\phi(n_i) = (p_i - 1)(q_i - 1)$. Therefore the key center is unable to compute the decryption keys $z_i = y_i^{-1}(\mathrm{mod}\,\phi(n_i))$ in order to decipher encrypted system messages. The inability of even the key center to decipher encrypted correspondence between members of its own system is a substantial security feature first introduced in the Winton Cryptosystem [14] in 2012 and retained in the Winton-Bass system.

Correspondence Protocol

Suppose that Bob and Sue are members of a Winton-Bass Cryptosystem network with system encryption matrix Q and system modulus n. Suppose further 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*, filling in trailing

alphabet characters as needed to obtain the maximum message length of $\alpha\beta$ characters in a manner that does not obscure the intended message when deciphered.

2. Bob separates m into α blocks $\{m_i\}_{i=1}^{\alpha}$ of β alphabet characters each.
3. For $1 \le i \le \alpha$, Bob converts m_i to its numerical equivalent $P_{ii} \le L$ using the scheme S.
4. Bob constructs the $\alpha \times \alpha$ diagonal matrix P with diagonal entries P_{ii} for $1 \le i \le \alpha$.
5. Bob enciphers P by computing $M = PQ \pmod{n}$.
6. Bob further enciphers M by computing $M^r \pmod{n}$.
7. Bob further enciphers M by computing $\left(M^r \pmod{n}\right)^e \pmod{k}$ and sends the result to Sue.
8. 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 is a diagonal matrix, then $M^r \pmod{n}$ is also a diagonal matrix with diagonal entries $\left\{\left[M^r \pmod{n}\right]_{ii}\right\}_{i=1}^{\alpha} = \{d_i\}_{i=1}^{\alpha}$. Then $\left(M^r \pmod{n}\right)^{ed} \pmod{k}$ is a diagonal matrix with diagonal entries $\left\{d_i^{ed} \pmod{k}\right\}_{i=1}^{\alpha}$. For $1 \le i \le \alpha$, d_i is a least residue modulo n, so that $d_i < n < k$, and so $k \nmid d_i$. Therefore $d_i^{ed} \pmod{k} = d_i \pmod{k}$ since $d = e^{-1} \pmod{\phi(k)}$ [13, Corollary 10]. Furthermore, $d_i \pmod{k} = d_i$ since $d_i < n < k$. Thus $\left(M^r \pmod{n}\right)^{ed} \pmod{k} = \left(M^r \pmod{n}\right) \pmod{k} = M^r \pmod{n}$.

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

Similar to step 8 above, since $[M^{ru} \pmod{n}]_{ii} < n < h$ and $b = c^{-1} \pmod{\phi(h)}$, then $\left(M^{ru} \pmod{n}\right)^{cb} \pmod{h} = \left(M^{ru} \pmod{n}\right) \pmod{h}$ [13, Corollary 10] $= M^{ru} \pmod{n}$.

12. Bob further deciphers the transmission by computing
$\left(M^{ru}(\bmod n)\right)^{t}$ (mod n) = $\left(M^{u}\right)^{rt}$ (mod n) = M^{u} (mod n).

Since M = PQ (mod n) then $M_{ii} < n$ for $1 \le i \le \alpha$, so that $n \nmid M_{ii}$. Thus either $p \nmid M_{ii}$ or $q \nmid M_{ii}$ since n = pq and $p \neq q$. Consequently either $p \nmid M_{ii}^{u}$ or $q \nmid M_{ii}^{u}$, and so $n \nmid M_{ii}^{u}$. Hence $\left(M_{ii}^{u}\right)^{rt}$ (mod n) = M_{ii}^{u} (mod n) since t = r^{-1} (mod ϕ(n)) [13, Corollary 10], and so $\left(M^{u}\right)^{rt}$ (mod n) = M^{u} (mod n).

Case 1: $h \le k$

13. Bob adds the digital signature for authenticating the identity of the sender by computing $\left(M^{u}(\bmod n)\right)^{b}$ (mod h).
14. Bob adds a layer of encryption by computing
$\left[\left(M^{u}(\bmod n)\right)^{b}(\bmod h)\right]^{e}(\bmod k)$ and sends the result to Sue.
15. Sue partially deciphers the transmission by computing
$\left[\left[\left(M^{u}(\bmod n)\right)^{b}(\bmod h)\right]^{e}(\bmod k)\right]^{d}(\bmod k) =$
$\left[\left(M^{u}(\bmod n)\right)^{b}(\bmod h)\right]^{ed}(\bmod k) = \left(M^{u}(\bmod n)\right)^{b}$ (mod h) as in step 8 since $[\left(M^{u}(\bmod n)\right)^{b}(\bmod h)]_{ii} < h \le k$ for $1 \le i \le \alpha$ and d = e^{-1} (mod ϕ(k)) [13, Corollary 10].
16. Sue continues deciphering the transmission by computing
$\left[\left(M^{u}(\bmod n)\right)^{b}(\bmod h)\right]^{c}(\bmod h) = \left(M^{u}(\bmod n)\right)^{bc}$ (mod h) =
M^{u} (mod n) as in step 11 since $[M^{u}(\bmod n)]_{ii} < n < h$ for $1 \le i \le \alpha$ and c = b^{-1} (mod ϕ(h)) [13, Corollary 10].

Case 2: $h > k$

13. Bob adds a layer of encryption by computing $\left(M^{u}(\bmod n)\right)^{e}$ (mod k).
14. Bob adds the digital signature for authenticating the identity of the sender by computing $\left[\left(M^{u}(\bmod n)\right)^{e}(\bmod k)\right]^{b}(\bmod h)$ and sends the result to Sue.
15. Sue partially deciphers the transmission by computing
$\left[\left[\left(M^{u}(\bmod n)\right)^{e}(\bmod k)\right]^{b}(\bmod h)\right]^{c}(\bmod h) =$

$\left[\left(M^{u}(\text{mod } n)\right)^{e}(\text{mod } k)\right]^{bc}(\text{mod } h) = \left(M^{u}(\text{mod } n)\right)^{e}$ (mod k) as in step 11 since $[\left(M^{u}(\text{mod } n)\right)^{e}(\text{mod } k)]_{ii} < k < h$ for $1 \le i \le \alpha$ and $c = b^{-1}(\text{mod } \phi(h))$ [13, Corollary 10].

16. Sue continues deciphering the transmission by computing $\left[\left(M^{u}(\text{mod } n)\right)^{e}(\text{mod } k)\right]^{d}(\text{mod } k) = \left(M^{u}(\text{mod } n)\right)^{ed}$ (mod k) = M^{u} (mod n) as in step 8 since $[M^{u}(\text{mod } n)]_{ii} < n < k$ for $1 \le i \le \alpha$ and $d = e^{-1}$ (mod $\phi(k)$) [13, Corollary 10].

Protocol Completion

17. In either case, Sue continues the deciphering process by computing $\left(M^{u}(\text{mod } n)\right)^{v}$ (mod n) = M^{uv} (mod n) = M (mod n) as in step 12 since $M_{ii} < n$ for $1 \le i \le \alpha$ and $v = u^{-1}$ (mod $\phi(n)$) [13, Corollary 10].

18. Sue completes the deciphering process by computing MQ^{-1} (mod n) = PQQ^{-1} (mod n) = P (mod n) = P since $P_{ii} \le L < n$ for $1 \le i \le \alpha$.

Since the diagonal entries $\{Q_{ii}\}_{i=1}^{\alpha}$ of Q are nonzero least residues modulo n and $\gcd\{Q_{ii}, n\} = 1$ for $1 \le i \le \alpha$, then Q_{ii}^{-1} (mod n) exists and is unique for $1 \le i \le \alpha$ [11, p. 139, Theorem 4.10]. Furthermore, the calculation of each Q_{ii}^{-1} (mod n) is achieved using an extended version of the Euclidean Algorithm [11, p. 141, Example 4.15]. Hence the $\alpha \times \alpha$ diagonal matrix with diagonal entries $\{Q_{ii}^{-1}(\text{mod } n\}_{i=1}^{\alpha}$ is Q^{-1} (mod n), so that $Q\,Q^{-1}$ (mod n) = $\mathbf{I}_{\alpha}$, the $\alpha \times \alpha$ identity matrix.

19. Sue next converts the diagonal entries $\{P_{ii}\}_{i=1}^{\alpha}$ of P to their alphabetic equivalents $\{m_{i}\}_{i=1}^{\alpha}$ using the scheme S.

20. Sue concatenates the character strings $\{m_{i}\}_{i=1}^{\alpha}$ to reconstruct and read Bob's message m.

The correspondence protocol of the Winton-Bass 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

$$\begin{tikzcd}
\text{Bob }(n,r,t;h,c,b) \qquad (h \le k) \arrow[d] & \text{Sue }(n,u,v;k,e,d) \\
m \arrow[d] & \\
P \arrow[d] & \\
PQ \text{ (mod n)}=M \arrow[d] & \\
M^{r} \text{ (mod n)} \arrow[d] & \\
\left(M^{r} \text{(mod n)}\right)^{e} \text{ (mod k)} \arrow[r] & \left(M^{r} \text{(mod n)}\right)^{e} \text{ (mod k)} \arrow[d] \\
& \left(M^{r} \text{(mod n)}\right)^{ed} \text{ (mod k)}= M^{r} \text{ (mod n)} \arrow[d] \\
& M^{ru} \text{ (mod n)} \arrow[d] \\
\left(M^{ru} \text{(mod n)}\right)^{c} \text{ (mod h)} \arrow[d] & \left(M^{ru} \text{(mod n)}\right)^{c} \text{ (mod h)} \arrow[l] \\
\left(M^{ru} \text{(mod n)}\right)^{cb} \text{ (mod h)}= M^{ru} \text{ (mod n)} \arrow[d] & \\
M^{rut} \text{ (mod n)}= M^{u} \text{ (mod n)} \arrow[d] & \\
\left(M^{u} \text{(mod n)}\right)^{b} \text{ (mod h)} \arrow[d] & \\
\left[\left(M^{u} \text{(mod n)}\right)^{b} \text{(mod h)}\right]^{e} \text{(mod k)} \arrow[r] & \left[\left(M^{u} \text{(mod n)}\right)^{b} \text{(mod h)}\right]^{e} \text{(mod k)} \arrow[d] \\
& \begin{array}{l} \left[\left(M^{u} \text{(mod n)}\right)^{b} \text{(mod h)}\right]^{ed} \text{(mod k)} = \\ \left(M^{u} \text{(mod n)}\right)^{b} \text{ (mod h)} \end{array} \arrow[d] \\
& \left(M^{u} \text{(mod n)}\right)^{bc} \text{ (mod h)}= M^{u} \text{ (mod n)} \arrow[d] \\
& M^{uv} \text{ (mod n)}=M \text{ (mod n)} \arrow[d] \\
& MQ^{-1} \text{ (mod n)}= PQQ^{-1} \text{ (mod n)}=P \arrow[d] \\
& m
\end{tikzcd}$$

Concluding Remarks

The encryption matrix Q in step 8 of the system structure is constructed so that the diagonal entries $\{Q_{ii}\}_{i=1}^{\alpha}$ of Q are distinct least residues modulo n which are relatively prime to n. Therefore each diagonal entry is nonzero and invertible modulo n. Thus Q is nonsingular modulo n, and Q^{-1}(mod n) is also a diagonal matrix with diagonal entries $[Q^{-1}(\text{mod}\, n)]_{ii} = Q_{ii}^{-1}$(mod n) for $1 \leq i \leq \alpha$. Furthermore, since the diagonal entries of Q are distinct, then identical diagonal entries of the matrix P constructed in step 4 of the correspondence protocol, which represent identical alphabetic character strings, are encrypted differently. Hence the Winton-Bass Cryptosystem is polyalphabetic [5, p. 45]. Also note that each diagonal entry of P numerically represents a block of β alphabet characters. Consequently the Winton-Bass Cryptosystem is polygraphic as well [5, p. 103]. Finally, since each of P, Q, and Q^{-1} is diagonal, then multiplication of these matrices modulo n in correspondence protocol steps 5 and 18 is accomplished by multiplying their corresponding diagonal entries and reducing each individual resulting diagonal entry modulo n. For example, the ii-entry of PQ (mod n) in protocol step 5 is simply $P_{ii}Q_{ii}$ (mod n).

Note that in step 9 of the system structure the primary encryption key 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 the primary decryption key $x_i = w_i^{-1}$(mod $\phi(n)$) calculated in step 10 is guaranteed [11, p. 139, Theorem 4.10]. Since the secondary encryption key y_i is selected in step 15 of the system structure such that $\gcd\{y_i, \phi(n_i)\} = 1$, a similar argument exists for the calculation of $z_i = y_i^{-1}$(mod $\phi(n_i)$) in step 16. Furthermore, the computation of x_i and z_i can be achieved using an extended version of the Euclidean Algorithm [11, p. 141, Example 4.15].

In step 1 of the correspondence protocol the sender is instructed to construct his message m using the alphabet *A*, filling in trailing alphabet characters as needed to obtain the maximum message length of $\alpha\beta$ characters in a manner that does not obscure the intended message when deciphered. One common manner by which this is accomplished is to complete the intended message m and add trailing X's until $\alpha\beta$ alphabet characters have been used.

In steps 13 and 14 of the correspondence protocol, the sender must determine the order in which to apply the exponents b and e based upon whether $h \leq k$ or $h > k$. Note that the moduli h and k are published in the key center directory. Therefore the information necessary for making such a decision is not only available to both the sender and recipient, but the sender and recipient are each required to use both h and k in the three-pass correspondence protocol. 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 $h = k$.

The EMO-2 and Winton Cryptosystems ([12],[14]) provide at least double encryption with each transmission in the three-pass protocol to make cryptanalysis by interceptors more difficult. However, the inclusion of the matrix encryption in step 5 of the Winton-Bass protocol, combined with the other encryptions similar to those of the Winton Cryptosystem, achieves at least triple encryption with each transmission. In fact, protocol step 10 actually results in a quadruple encryption before Sue transmits to Bob. While it may appear that the exponentiations performed in protocol steps 13 and 14 produce another quadruple encryption, this is not the case. For h and $c = b^{-1} (\text{mod } \phi(h))$ are published, making it 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, but instead serves as the digital signature by which the recipient can verify the sender's identity [11, p. 300]. For if the recipient applies the sender'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 the sender's private decryption key known only by the sender. Consequently the sender's identity is authenticated by the recipient.

Similar to the EMO-2 and Winton Cryptosystems ([12],[14]), 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]). 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 [5, pp. 157-158, Question 4]. Consequently, even if an interceptor gains access to the system modulus n and network member's private primary encryption key, say w_j, the interceptor cannot compute the network member's corresponding key $x_j = w_j^{-1} (\text{mod } \phi(n))$ for decryption purposes. The key center, however, knows the keys $\{x_i\}$, and thus has the ability to remove an encryption produced with the key w_j.

In contrast, and similar to the Winton Cryptosystem [14], each secondary encryption key y_i has a corresponding decryption key z_i known only to the network member who selects y_i. Furthermore, that network member's corresponding modulus $n_i = p_i q_i$ has prime factors p_i and q_i known only to that member. Therefore even though n_i is published, it is difficult for anyone else to factor $n_i = p_i q_i$, and thus to compute $\phi(n_i) = (p_i - 1)(q_i - 1)$, whenever n_i is sufficiently large. Consequently, even with n_i and y_i being published, the key $z_i = y_i^{-1} (\text{mod}\, \phi(n_i))$ 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.

The correspondence protocol of the Winton-Bass Cryptosystem is accomplished by successive exponentiations relative to different moduli. Furthermore, although $\left[a^r (\mathrm{mod}\, n)\right]^t (\mathrm{mod}\, n) \equiv a^{rt} (\mathrm{mod}\, n)$, in general we have $\left[a^r (\mathrm{mod}\, n_1)\right]^t (\mathrm{mod}\, n_2) \not\equiv \left[a^t (\mathrm{mod}\, n_2)\right]^r (\mathrm{mod}\, n_1)$. Note however that all the moduli (n and $\{n_i\}$) used in the three-pass protocol are published, and thus are accessible by all network members. As a result, 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 is 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, similar to the Winton Cryptosystem [14], the decryption process in the Winton-Bass Cryptosystem is based on results established in 2009 by Richard A. Winton [13] rather than Euler's Theorem. More specifically, the selection of the prime factors p and q of the primary modulus n require only that $n = pq > L$
([13, Theorem 8],[13, Corollary 10]). Hence the network modulus n of the Winton-Bass 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 prime factors $\{p_i\}$ and $\{q_i\}$ for the individual secondary moduli $\{n_i\}$. Consequently, these substantially smaller moduli enable the Winton-Bass Cryptosystem to operate with a greater computational efficiency than the EMO-1 and EMO-2 systems.

† *Richard Winton*, *Ph.D.*, Tarleton State University, USA
‡ *Jeremiah Bass, Ph.D.*, Tarleton State University, 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 Identity*, 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 Identity*, Journal of 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 Association for Computing Machinery, 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.
14. R. A. Winton, *Combining Public and Private Key Cryptography*, Journal of Mathematical Sciences and Mathematics Education, Vol. 7, No. 1, (2012) pp. 1-10.