The Cocks IBE Scheme: The Legendre Symbol and Quadratic Reciprocity

Shannon Prager
University of Redlands

Follow this and additional works at: https://inspire.redlands.edu/cas_honors

Part of the Applied Mathematics Commons, Mathematics Commons, and the Statistics and Probability Commons

Recommended Citation
The Cocks IBE Scheme:

The Legendre Symbol and Quadratic Reciprocity

By: Shannon Prager
# Table of Contents

Introduction ......................................................................................... 3  
Section 1: Basic Concepts in Number Theory. ....................................... 4  
  1.1 Law of Quadratic Reciprocity ......................................................... 14  
  1.2 Proof of LQR ........................................................................... 21  
Section 2: Cryptography ..................................................................... 25  
  2.1 Public-key Cryptography .............................................................. 26  
  2.2 Identity-based Encryption ............................................................ 28  
Section 3: Cocks IBE Scheme .............................................................. 31  
  3.1 Set-up ..................................................................................... 31  
  3.2 Encryption ............................................................................ 37  
  3.3 Decryption ............................................................................ 38  
  3.4 Problems ............................................................................. 38  
  3.5 Security ............................................................................... 39  
  3.5.1 Security Proof ................................................................ 40  
  3.5 Example ............................................................................ 42  
Conclusion .......................................................................................... 45  
References ........................................................................................ 46
Introduction

The Cocks IBE Scheme was first proposed by Clifford Cocks in 2001 at the 8th IMA International Conference on Cryptography and Coding. It is a cryptosystem that allows identity-based encryption (IBE) and is based on the difficulty of the composite quadratic residue problem, which has to do with when a number is a square modulo a positive integer $n$. [3] An identity-based encryption scheme is a type of public-key cryptosystem where the public key is some unique information about the identity of the user (e.g. a user's email address or important dates in his/her life). [5]

This cryptosystem depends on the sender and receiver knowing solutions to public quadratic equations modulo a large composite number $M$, where $M$ is the product of two very large primes, $P$ and $Q$. Both $P$ and $Q$ are usually 600-700 digits, making $M$ extremely large, and factorization of $M$ nearly impossible. This, in part, makes the Cocks IBE Scheme a very secure system, and it can be shown, as is proved later in this paper, that being able to crack the scheme would be equivalent to solving the composite quadratic residue problem, which is currently unsolved.
Section 1: Basic Concepts in Number Theory

A major component of understanding the Cocks IBE scheme is the Law of Quadratic Reciprocity. Topics from number theory needed in order to understand and prove this theorem include: modular arithmetic, linear congruences, quadratic residues, Euler's Criterion, the Legendre symbol, theorems for calculating the Legendre symbol, the Jacobi symbol, and Gauss's Lemma.

Modular arithmetic will be the main form of arithmetic used in this paper. In particular, we will be using linear congruences very often and looking at when two integers are congruent to each other.

Definition 1.1: If \( a, b \in \mathbb{Z} \) and \( n \in \mathbb{N} \), we say that \( a \) is congruent to \( b \) modulo \( n \) if \( n \mid (a-b) \), and write \( a \equiv b \pmod{n} \). [1, pg. 22]

For all theorems and definitions from this point on, we will assume that \( a \) is an integer and \( p \) is an odd prime.

Theorem 1.1: Let \( p, q \) be distinct primes. If \( p \mid a \) and \( q \mid a \) and \( \gcd(p, q) = 1 \), then \( pq \mid a \).

Proof: Since \( p \mid a \) and \( q \mid a \), then \( a = p \cdot k \) and \( a = q \cdot l \) for some integers \( q, l \). Then, \( p \cdot k = q \cdot l \). Therefore, \( p \mid ql \). By theorem, if \( \gcd(p, q) = 1 \) and \( p \mid ql \), then \( p \mid l \). We know that \( \gcd(p, q) = 1 \) since \( p \) and \( q \) are distinct primes; thus, we can conclude that \( p \mid l \). Then \( l = p \cdot m \) for some integer \( m \). Therefore, \( a = p \cdot k = q \cdot l = q \cdot p \cdot m = pqm \).

Thus, \( a = pqm \), and therefore \( pq \mid a \). \( \blacksquare \)
**Definition 1.2:** An integer \( a \) is a *quadratic residue* modulo an odd prime \( p \) if:

1) \( x^2 \equiv a \pmod{p} \) has an integer solution \( x \), and

2) \( \gcd(a, p) = 1 \) \[1, pg. 115\]

For example, 2 is a quadratic residue, or square mod 7. To see this, we need to solve the congruence \( x^2 \equiv 2 \pmod{7} \). Note that \( \gcd(2, 7) = 1 \). We can easily see that both \( x = 3 \) and \( x = 4 \) are solutions, since \( 3^2 = 9 \equiv 2 \pmod{7} \) and \( 4^2 = 16 \equiv 2 \pmod{7} \). The following theorem introduces a simpler way to check whether \( a \) is a quadratic residue modulo \( p \).

**Theorem 1.2-Euler's Criterion:** The integer \( a \) is a quadratic residue modulo an odd prime \( p \) if and only if \( a^{(p-1)/2} \equiv 1 \pmod{p} \). \[1, pg. 116\]

To prove this theorem, we first need to remind ourselves of several definitions and theorems.

**Definition 1.3:** Let \( n \in \mathbb{N} \). If \( h \) is the smallest positive integer such that \( a^h \equiv 1 \pmod{n} \), we say that \( h \) is the *order* of \( a \) modulo \( n \). \[1, pg. 93\]

**Theorem 1.3:** Let \( m \in \mathbb{N} \). If \( a \) has order \( h \) modulo \( m \), and \( a^r \equiv 1 \pmod{m} \), then \( h | r \).

*Proof:* By Euclid's division lemma, there exist \( k, s \in \mathbb{Z} \) such that \( r = kh + s \) (\( 0 \leq s < h \)). Hence, \( 1 \equiv a^r = a^{kh+s} = (a^h)^k a^s \equiv 1^k a^s = a^s \pmod{m} \). Thus \( s = 0 \), since \( h \) is the least positive exponent such that \( a^h \equiv 1 \pmod{m} \) and \( s \geq 0 \). Therefore, \( h | r \). \[1, pg. 94\]
Definition 1.4: Let \( m \in \mathbb{N} \). The function \( \phi(m) \) shall denote the number of positive integers less than \( m \) that are relatively prime to \( m \). This function \( \phi(m) \) is called the Euler \( \phi \)-function.

[1, pg. 54]

Definition 1.5: Let \( m \in \mathbb{N} \). If \( g \) has order \( \phi(m) \) modulo \( m \), then \( g \) is called a primitive root modulo \( m \).

[1, pg. 94]

Theorem 1.4.1: If \( g \) is a primitive root, then \( g, g^2, \ldots, g^{\phi(m)} \) are all distinct and thus include all elements modulo \( m \) relatively prime to \( m \). That is, \( g \) is a generator mod \( m \).

Theorem 1.4.2: Let \( m \in \mathbb{N} \). Then \( m \) has primitive roots if and only if \( m \) is 2 or 4 or a number of the form \( p^2 \) or \( 2p^2 \), where \( p \) denotes an odd prime.

[1, pg. 97]

Theorem 1.5 (Fermat’s Little Theorem): If \( p \) is a prime and \( \gcd(n, p) = 1 \), then

\[
n^{p-1} \equiv 1 \pmod{p}.
\]

[1, pg. 62]

Now we have the necessary means to prove Euler’s Criterion.

Proof of Euler’s Criterion: Suppose that \( a \) is a quadratic residue modulo \( p \). Let \( X \) be any integer such that

\[
X^2 \equiv a \pmod{p}.
\]

Since \( \gcd(p, a) = 1 \), then \( \gcd(X^2, a) = 1 \), and thus \( \gcd(X, p) = 1 \). Consequently,

\[
a \frac{p-1}{2} \equiv (X^2)^{\frac{p-1}{2}} \equiv X^{p-1} \equiv 1 \pmod{p},
\]

by Fermat’s Little Theorem.

On the other hand, suppose that
\[ a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \]

Let \( g \) be a primitive root modulo \( p \). Since \( g \) is a primitive root, then \( g \) generates everything in the group \( \mathbb{Z}_p^* \), which includes every integer that is relatively prime to \( p \), and there exists some power, \( r \), of \( g \), such that

\[ g^r \equiv a \pmod{p}, \]

and so,

\[ (g^r)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \]

Since \( g \) is a primitive root, it has order \( p - 1 \). But, from Theorem 1.3, we see that

\((p - 1) | (r(p - 1)/2). Thus, r/2 must be an integer; that is, \( r = 2s \), where \( s \) is an integer.

Hence, if \( x = g^s \), then

\[ x^2 = g^{2s} = g^r \equiv a \pmod{p}; \]

this establishes Euler's Criterion. \( \blacksquare \)

[1, pg. 116]

This proof leads us to a useful corollary.

**Corollary 1.1:** Let \( g \) be a primitive root modulo \( p \), and assume \( \gcd(a, p) = 1 \). Let \( r \) be any integer such that \( g^r \equiv a \pmod{p} \). Then \( r \) is even if and only if \( a \) is a quadratic residue modulo \( p \)

[1, pg. 116]

**PROOF:** Assuming that \( a \) is a quadratic residue modulo \( p \), we can see that \( r \) is even from the proof of Euler's criterion. Conversely, if we assume that \( r \) is even, then \( r = 2s \), and thus \( g^r = g^{2s} = (g^s)^2 \equiv a \pmod{p} \). Therefore, \( a \) is a square, or quadratic residue modulo \( p \).

Now we can look at an example of Euler's Criterion. Let \( a = 2, p = 5 \). Then
\[ \frac{\phi - 1}{2} = 2^2 = 4 \neq 1 \pmod{5}. \] Therefore, by Euler's Criterion, 2 is not a quadratic residue modulo 5. We can confirm this by looking at all the elements of \( \mathbb{Z}_5 \) and checking whether they square to 2. We note that \( 0^2 = 0 \equiv 0 \pmod{5}, 1^2 = 1 \equiv 1 \pmod{5}, 2^2 = 4 \equiv 4 \pmod{5}, 3^2 = 9 \equiv 4 \pmod{5}, 4^2 = 16 \equiv 1 \pmod{5}. \) Therefore, none of the elements square to be congruent to 2 modulo 5, and thus, 2 is not a quadratic residue modulo 5.

We shall now define the Legendre Symbol, as well as the Jacobi Symbol, both of which greatly simplify calculations in problems on quadratic residues, and are needed in order to prove the Law of Quadratic Reciprocity.

**Definition 1.6:** The Legendre Symbol is defined as:

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue modulo } p \\
0 & \text{if } p \mid a \\
-1 & \text{otherwise}
\end{cases} \quad [1, \text{pg. 116}]
\]

By this definition, using the same example from above, we can see that \( \left( \frac{2}{7} \right) = 1 \) since 2 is a quadratic residue mod 7. We can see that \( \left( \frac{6}{3} \right) = 0 \) since 3|6 and thus, 6 is not a quadratic residue mod 3. Also, as previously mentioned, 2 is not a quadratic residue modulo 5 and 5|2; therefore \( \left( \frac{2}{5} \right) = -1. \)

**Theorem 1.6:** If \( p \) is an odd prime and \( a \) and \( b \) are relatively prime to \( p \), then

\[
\left( \frac{a}{p} \right) = \left( \frac{b}{p} \right), \text{if } a \equiv b \pmod{p} \quad (1.6.1)
\]

\[
\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \quad (1.6.2)
\]
\[ a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p} \]  

(1.6.3)

[1, pg. 117]

Proof: Statement (1.6.1) follows directly from the definition of \( \left(\frac{a}{p}\right) \).

Statement (1.6.2) follows from Corollary 1.1. First, let \( a \equiv g^r \pmod{p} \) and \( b \equiv g^s \pmod{p} \). Then \( ab \equiv g^r g^s = g^{r+s} \pmod{p} \). There are three different cases for the possible values of \( \left(\frac{a}{p}\right) \) and \( \left(\frac{b}{p}\right) \) and we will look at each one separately.

Case 1: Let both \( \left(\frac{a}{p}\right) \) and \( \left(\frac{b}{p}\right) \) equal \( 1 \). Then \( \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = 1 \). Also, both \( a \) and \( b \) are quadratic residues modulo \( p \), and thus by Corollary 1.1, both \( r \) and \( s \) are even. Therefore, \( r + s \) is even, and thus, \( ab \), which is congruent to \( g^{r+s} \pmod{p} \), is a quadratic residue modulo \( p \) and \( \left(\frac{ab}{p}\right) = 1 \). Therefore, \( \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \).

Case 2: Let \( \left(\frac{a}{p}\right) = 1 \) and \( \left(\frac{b}{p}\right) = -1 \). Then \( \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = -1 \). Also, \( a \) is a quadratic residue, whereas \( b \) is not, and thus by Corollary 1.1, \( r \) is even and \( s \) is odd. Therefore, \( r + s \) is odd, and thus, \( ab \), which is congruent to \( g^{r+s} \pmod{p} \), is not a quadratic residue modulo \( p \) by Corollary 1.1 and \( \left(\frac{ab}{p}\right) = -1 \). Therefore, \( \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \). Similarly, we can see that if \( \left(\frac{a}{p}\right) = -1 \) and \( \left(\frac{b}{p}\right) = 1 \), then the same proof would hold and we would also have \( \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \).

Case 3: Let both \( \left(\frac{a}{p}\right) \) and \( \left(\frac{b}{p}\right) \) equal \( -1 \). Then \( \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = 1 \). Also, both \( a \) and \( b \) are not quadratic residues modulo \( p \), and thus by Corollary 1.1, both \( r \) and \( s \) are odd. Therefore,
\( r + s \) is even, and thus, \( ab \), which is congruent to \( g^{r+s} \) (mod \( p \)) is a quadratic residue modulo \( p \) by Corollary 1.1 and \( \left( \frac{ab}{p} \right) = 1 \). Therefore, \( \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \left( \frac{ab}{p} \right) \).

Therefore, \( \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \left( \frac{ab}{p} \right) \) for all possible values of \( \left( \frac{a}{p} \right) \) and \( \left( \frac{b}{p} \right) \).

As for (1.6.3), we see that if \( a \) is a quadratic residue modulo \( p \), then Euler’s Criterion implies that

\[
a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.
\]

Since

\[
a^{p-1} \equiv 1 \pmod{p}
\]

by Euler’s Criterion, then raising both sides of the congruence to a power of \( \frac{1}{2} \), we can see that

\[
a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p},
\]

since \( p \nmid a \). Thus, if \( \gcd(a, p) = 1 \) and \( a \) is not a quadratic residue modulo \( p \), then, by Euler’s Criterion, we see that

\[
a^{\frac{p-1}{2}} \equiv -1 = \left( \frac{a}{p} \right) \pmod{p}.
\]

\[\text{[1, pp. 117-118]}\]

**Definition 1.7:** If \( n \) is any integer, then the least residue of \( n \) modulo \( m \), where \( m \) is a positive integer, is the integer \( x \) in the interval \( \left( -\frac{m}{2} \right., \, \frac{m}{2} \right] \) such that \( n \equiv x \pmod{m} \). We denote the least residue of \( n \) modulo \( m \) by \( LR_m(n) \).

\[\text{[1, pg. 119]}\]
For example, the set \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\} is a complete set of least residues modulo 11. Thus \( LR_{11}(21) = -1 \), since \( 21 \equiv -1 \pmod{11} \); similarly, \( LR_{11}(99) = 0 \), and \( LR_{11}(60) = 5 \).

For \( p \) an odd prime, the complete set of least residues mod \( p \) is
\[
\left\{ \frac{p-1}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{p-3}{2}, \frac{p-1}{2} \right\}
\]

**Theorem 1.7- Gauss's Lemma:** Let \( \gcd(m, p) = 1 \) where \( p \) is an odd prime and \( m \in \mathbb{Z} \), and let \( \mu \) be the number of integers in the set
\[
\left\{ m, 2m, \ldots, \frac{1}{2}(p - 1)m \right\}
\]
whose least residues modulo \( p \) are negative. Then \( \left( \frac{m}{p} \right) = (-1)^\mu \). [1, pg. 119]

Before proving this theorem, we must first define the signum of \( x \) and state the cancellation law.

**Definition 1.8:** We define \( \text{sgn}(x) \) (read signum of \( x \)), where \( x \) is a real number, by
\[
\text{sgn}(x) = \begin{cases} 
+1 & \text{if } x > 0, \\
0 & \text{if } x = 0 \\
-1 & \text{if } x < 0 
\end{cases}
\]
In general, we note that \( x = |x| \, \text{sgn}(x) \). [1, pg. 119]

**Theorem 1.8- Cancellation Law:** For \( b, d, d' \in \mathbb{Z} \) and \( c \in \mathbb{Z}^+ \), if \( bd \equiv bd' \pmod{c} \) and \( \gcd(b, c) = 1 \), then \( d \equiv d' \pmod{c} \).
Proof: Since \((bd - bd')/c\) is an integer, \(c|b(d - d')\). Thus, since \(c\) and \(b\) are relatively prime, \(c|(d - d')\), that is, \(d \equiv d' \pmod{c}\). □

We give the proof from Andrews' text. [1, pp. 119-120]

Proof of Gauss’s Lemma: First note that none of the integers \(m, 2m, ..., \frac{1}{2} (p - 1)m\) is divisible by \(p\) since \(\gcd(m, p) = 1\). Now, for any integer \(n\),

\[nm \equiv LR_p(nm) = \text{sgn} \left( LR_p(nm) \right) |LR_p(nm)| \pmod{p}.\]

We also know that the value \(|LR_p(nm)|\) is distinct for different \(n\) values. That is, for integers \(n_1, n_2\), \(|LR_p(n_1 m)| \neq |LR_p(n_2 m)|\). There are two cases where \(|LR_p(n_1 m)| = |LR_p(n_2 m)|:

Case 1: If \(n_1 m \equiv n_2 m \pmod{p}\), where \(\gcd(m, p) = 1\), then \(n_1 \equiv n_2 \pmod{p}\) by Theorem 1.8.

Case 2: If \(n_1 m \equiv -n_2 m \pmod{p}\), where \(\gcd(m, p) = 1\), then \(n_1 \equiv -n_2 \pmod{p}\) by Theorem 1.8. Therefore, \(n_1 + n_2 \equiv 0 \pmod{p}\). Thus, \(p|(n_1 + n_2)\). But \(0 < n_1 \leq \frac{p-1}{2}\) and \(0 < n_2 \leq \frac{p-1}{2}\), thus \(0 < n_1 + n_2 \leq p - 1\), but this contradicts the fact that \(p|(n_1 + n_2)\), and therefore, \(|LR_p(n_1 m)| \neq |LR_p(n_2 m)|\).

Therefore, \(|LR_p(nm)|\) is distinct for different \(n\) values.

Since \(0 < |LR_p(nm)| < p/2\), we see that as \(n\) takes all integral values in the interval \((0, p/2)\), so does \(|LR_p(nm)|\). Consequently,

\[m(2m)(3m)...\left(\frac{p - 1}{2} \frac{m}{2}\right) \equiv \text{sgn} \left( LR_p(m) \right) \text{sgn}(LR_p(2m))...\text{sgn} \left( LR_p \left( \frac{p - 1}{2} \frac{m}{2} \right) \right)\]

\[\times \left[ |LR_p(m)| \cdot |LR_p(2m)|...|LR_p \left( \frac{p - 1}{2} \frac{m}{2} \right) | \right] \pmod{p},\]

12
or

\[
\left(\frac{1}{2} (p - 1)\right)! m^{p-1} \equiv \text{sgn}(LR_p(m)) \text{sgn}(LR_p(2m)) \ldots \text{sgn}(LR_p\left(\frac{1}{2} (p - 1)m\right)) \cdot \left(\frac{1}{2} (p - 1)\right)! \pmod{p}.
\] (1.7.1)

Since \(\left(\frac{1}{2} (p - 1)\right)!\) is relatively prime to \(p\), we may cancel it from both sides of (1.7.1).

Hence,

\[
m^{p-1} \equiv \text{sgn}(LR_p(m)) \text{sgn}(LR_p(2m)) \ldots \text{sgn}(LR_p\left(\frac{1}{2} (p - 1)m\right)) \pmod{p}.
\]

But \(m^{p-1} \equiv \left(\frac{m}{p}\right) \pmod{p}\), by Theorem (1.6.3), and

\[
(-1)^\mu = \text{sgn}(LR_p(m)) \text{sgn}(LR_p(2m)) \ldots \text{sgn}(LR_p\left(\frac{1}{2} (p - 1)m\right)).
\]

Thus,

\[
\left(\frac{m}{p}\right) \equiv (-1)^\mu \pmod{p}
\]

Since each of the congruence equals either +1 or -1, and since \(p > 2\),

\[
\left(\frac{m}{p}\right) = (-1)^\mu. \quad \blacksquare
\] [1, pp. 119-120]

We can extend the definition of the symbol \(\left(\frac{a}{m}\right)\) to include the case where \(m\) is any odd number:

**Definition 1.9:** If \(m = p_1 p_2 \ldots p_r\) where the \(p_i\) are odd primes (not necessarily distinct),

then the Jacobi Symbol \(\left(\frac{n}{m}\right)\), \(n \in \mathbb{N}\), is defined as

\[
\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right) \left(\frac{n}{p_2}\right) \ldots \left(\frac{n}{p_r}\right).
\] [1, pg. 118]
It is useful to note that \( \left( \frac{n}{m} \right) = 1 \) does not imply that \( n \) is a square, or quadratic residue, mod \( m \) like \( \left( \frac{n}{p} \right) = 1 \) does, where \( p \) is an odd prime. This is because \( \left( \frac{n}{m} \right) \) is the product of many Legendre Symbols that take on the value 1, \(-1\), or 0 depending on the conditions explained in Definition 1.6.

For example, \( \left( \frac{5}{6} \right) = 1 \) but 5 is not a quadratic residue mod 6. That is, there is no \( x \) such that \( x^2 \equiv 5 \pmod{6} \). To see this, we can look at all the elements in \( \mathbb{Z}_6 \) and see if any of them square to 5:

\[
\begin{align*}
1^2 &= 1 \equiv 1 \pmod{6} \\
2^2 &= 4 \equiv 4 \pmod{6} \\
3^2 &= 9 \equiv 3 \pmod{6} \\
4^2 &= 16 \equiv 4 \pmod{6} \\
5^2 &= 25 \equiv 1 \pmod{6},
\end{align*}
\]

Therefore, none of elements square to 5, and thus 5 is not a quadratic residue mod 6.

### 1.1 The Law of Quadratic Reciprocity

The Law of Quadratic Reciprocity enables us to solve almost all quadratic congruences involving a prime modulus. It is by no means an easy theorem; great mathematicians such as L. Euler and A. Legendre were perplexed by it. It shows the measure of greatness of C.F. Gauss that he proved it when he was only nineteen years old. Since this theorem is of fundamental importance in number theory, Gauss returned to study it several times throughout his life, and he gave at least six different proofs. [1, pg. 118] We will give one of these proofs in detail in the next section.
**Theorem 1.9- Law of Quadratic Reciprocity (LQR):** If \( p \) and \( q \) are distinct odd primes, then \( \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) \) unless \( p \equiv q \equiv 3 \pmod{4} \), in which case \( \left( \frac{p}{q} \right) = -\left( \frac{q}{p} \right) \).

**REMARKS:** This theorem may be stated equivalently in the form

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4}
\]

[1, pg. 116]

Also, this theorem generalizes to the case where \( p \) and \( q \) are only distinct positive odd integers, not necessarily prime [4, pg. 28].

For example, pick two distinct primes, 5 and 11. By the LQR, since

\[
5 \equiv 1 \pmod{4} \quad \text{and} \quad 11 \equiv 3 \pmod{4},
\]

then \( \left( \frac{5}{11} \right) = \left( \frac{11}{5} \right) \). One of the primes can be

\[
\equiv 3 \pmod{4};
\]

they just cannot both be. To check this, we can compute the values of

\[
\left( \frac{5}{11} \right) \quad \text{and} \quad \left( \frac{11}{5} \right).
\]

To compute the value of \( \left( \frac{5}{11} \right) \), we check to see if 5 is a quadratic residue modulo 11. This involves solving the equation \( x^2 \equiv 5 \pmod{11} \). It is simple to see that \( x = 4 \) is a solution since \( 4^2 = 16 \equiv 5 \pmod{11} \). Therefore, \( \left( \frac{5}{11} \right) = 1 \) using the Legendre Symbol. Similarly, we check to see if 11 is a quadratic residue modulo 5. We solve the equation \( x^2 \equiv 11 \pmod{5} \) or \( x^2 \equiv 1 \pmod{5} \) since 11 \( \equiv 1 \pmod{5} \). We can see that \( x = 1 \) is a solution since \( 1^2 = 1 \equiv 1 \pmod{5} \). Thus \( \left( \frac{11}{5} \right) = 1 \) by the definition of the Legendre Symbol, and thus \( \left( \frac{5}{11} \right) = \left( \frac{11}{5} \right) \).

**Theorem 1.10:** If \( p \) is an odd prime, then
\[ (-1)^{a(p)} = (-1)^{\frac{p-1}{2}} \quad (1.10.1) \]

\[ (2)^{a(p)} = (-1)^{\frac{p^2-1}{2}} \quad (1.10.2) \]

\[ (3)^{a(p)} = \begin{cases} 
1 & \text{if } p \equiv 1 \text{ or } 11 \pmod{12} \\
-1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{12} 
\end{cases} \quad (1.10.3) \]

Proof: By Gauss’s Lemma, with \( m = -1 \), we see that \( \mu = \frac{1}{2} (p - 1) \) since

\(-1, -2, \ldots, -\frac{1}{2} (p - 1) \) all have negative least residues; this establishes (1.10.1).

With \( m = 2 \), \( \mu \) is the number of integers in the set \( \{2, 4, \ldots, p - 1\} \) whose least residues modulo \( p \) are negative, which is the same as the number of even integers in the interval \( \left[ \frac{p+1}{2}, p - 1 \right] \). Since positive residues take on values between 0 and \( \frac{p-1}{2} \), then any number greater than \( \frac{p-1}{2} \) must have a negative residue. There are \( \frac{p-1}{2} \) elements in the set \( \{2, 4, \ldots, p - 1\} \). The value \( \frac{p-1}{2} \) can either be even or odd, depending on the value of \( p \). If \( \frac{p-1}{2} \) is even, then the set \( \{2, 4, \ldots, p - 1\} \) can be split in the two sets \( \{2, 4, \ldots, \frac{p-1}{2}\} \) and \( \left\{ \frac{p+1}{2}, \ldots, p - 1 \right\} \), with the former having positive least residues, and the latter having negative least residues. The set \( \{2, 4, \ldots, \frac{p-1}{2}\} \) has \( \frac{p-1}{4} \) elements, thus, the set \( \left\{ \frac{p+3}{2}, \ldots, p - 1 \right\} \) has \( \frac{p-1}{4} \) elements. If \( \frac{p-1}{2} \) is odd, then the set \( \{2, 4, \ldots, p - 1\} \) can be split into the two sets \( \{2, 4, \ldots, \frac{p-3}{2}\} \) and \( \left\{ \frac{p+1}{2}, \ldots, p - 1 \right\} \), with the former having positive least residues, and the latter having negative least residues. The set \( \{2, 4, \ldots, \frac{p-3}{2}\} \) has \( \frac{p-3}{4} \) elements, thus, the set \( \left\{ \frac{p+1}{2}, \ldots, p - 1 \right\} \) has \( \frac{p-3}{4} \) elements.

We will now look at possible values of \( p \) and what \( \mu \) equals for these values.
Case 1: Let \( p = 8s + 1 \) for some integer \( s \). Then \( \frac{p-1}{2} = \frac{8s + 1 - 1}{2} = 4s \), which is even.

Therefore, the number of elements in the set of negative least residues is

\[
\frac{p-1}{2} - \frac{p-1}{4} = \frac{8s + 1 - 1}{2} - \frac{8s + 1 - 1}{4}
\]

\[
= \frac{8s}{2} - \frac{8s}{4}
\]

\[
= 4s - 2s = 2s.
\]

Case 2: Let \( p = 8s + 3 \) for some integer \( s \). Then \( \frac{p-1}{2} = \frac{8s + 3 - 1}{2} = \frac{8s + 2}{2} = 4s + 1 \), which is odd. Therefore, the number of elements in the set of negative least residues is

\[
\frac{p-1}{2} - \frac{p-3}{4} = \frac{8s + 3 - 1}{2} - \frac{8s + 3 - 3}{4}
\]

\[
= \frac{8s + 2}{2} - \frac{8s}{4}
\]

\[
= 4s + 1 - 2s = 2s + 1.
\]

Case 3: Let \( p = 8s + 5 \) for some integer \( s \). Then \( \frac{p-1}{2} = \frac{8s + 5 - 1}{2} = \frac{8s + 4}{2} = 4s + 2 \), which is even. Therefore, the number of elements in the set of negative least residues is

\[
\frac{p-1}{2} - \frac{p-1}{4} = \frac{8s + 5 - 1}{2} - \frac{8s + 5 - 1}{4}
\]

\[
= \frac{8s + 4}{2} - \frac{8s + 4}{4}
\]

\[
= 4s + 2 - (2s + 1) = 2s + 1.
\]

Case 4: Let \( p = 8s + 7 \) for some integer \( s \). Then \( \frac{p-1}{2} = \frac{8s + 7 - 1}{2} = \frac{8s + 6}{2} = 4s + 3 \), which is odd. Therefore, the number of elements in the set of negative least residues is

\[
\frac{p-1}{2} - \frac{p-3}{4} = \frac{8s + 7 - 1}{2} - \frac{8s + 7 - 3}{4}
\]

\[
= \frac{8s + 6}{2} - \frac{8s + 4}{4}
\]
Thus,
\[
\mu = \begin{cases} 
2s & \text{when } p = 8s + 1 \\
2s + 1 & \text{when } p = 8s + 3 \\
2s + 1 & \text{when } p = 8s + 5 \\
2s + 2 & \text{when } p = 8s + 7.
\end{cases}
\]

Hence, \( \mu \) is even if and only if \( p \equiv \pm 1 \pmod{8} \). Consequently,
\[
\left( \frac{2}{p} \right) = \begin{cases} 
1 & \text{when } p \equiv \pm 1 \pmod{8} \\
-1 & \text{when } p \equiv \pm 3 \pmod{8}.
\end{cases}
\]

We can see that \(( -1 )^{\frac{p^2 - 1}{8}} = \begin{cases} 
1 & \text{when } p \equiv \pm 1 \pmod{8}, \\
-1 & \text{when } p \equiv \pm 3 \pmod{8}.
\end{cases}\)

This is true since \( p \equiv \pm 1 \pmod{8} \) means \( p = \pm 1 + 8k \) for some \( k \in \mathbb{Z} \) and thus,
\[
(-1)^{\frac{p^2 - 1}{8}} = (-1)^{\frac{(\pm 1 + 8k)^2 - 1}{8}}
\]
\[
= (-1)^{\frac{1 \pm 16k + 64k^2 - 1}{8}}
\]
\[
= (-1)^{\frac{\pm 16k + 64k^2}{8}}
\]
\[
= (-1)^{\pm 2k + 8k^2}
\]
\[
= (-1)^{2(\pm k + 4k^2)}
\]
The value \( 2(\pm k + 4k^2) \) will always yield an even integer and \(-1\) to an even power equals \(1\). Therefore, \((-1)^{\frac{p^2 - 1}{8}} = (-1)^{2(\pm k + 4k^2)} = 1 \) whenever \( p \equiv \pm 1 \pmod{8} \).

Similarly, \( p \equiv \pm 3 \pmod{8} \) means \( p = \pm 3 + 8k \) for some \( k \in \mathbb{Z} \) and thus,
\[
(-1)^{\frac{p^2 - 1}{8}} = (-1)^{\frac{(\pm 3 + 8k)^2 - 1}{8}}
\]
\[
= (-1)^{\frac{9 \pm 48k + 64k^2 - 1}{8}}
\]
\[
= (-1)^{\frac{8 \pm 16k + 54k^2}{8}}
\]
The value $1 \pm 2(3k + 4k^2)$ will always yield an odd number and $-1$ to an odd power equals $-1$. Therefore, $(-1)^{p^2 - 1} = (-1)^{1\pm 2(3k+4k^2)} = -1$ whenever $p \equiv \pm 3 \pmod{8}$.

Therefore, (1.10.2) is established.

For (1.10.3), we know that

$$\left( \frac{3}{p} \right) = \begin{cases} 
\left( \frac{3}{3} \right) & \text{if } p \equiv 1 \pmod{4} \\
-\left( \frac{3}{p} \right) & \text{if } p \equiv 3 \pmod{4}.
\end{cases}$$

by the LQR.

We also know that

$$\left( \frac{p}{3} \right) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{3} \\
-1 & \text{if } p \equiv 2 \pmod{3}.
\end{cases}$$

If we want $\left( \frac{3}{p} \right) = 1$, then we want $p \equiv 1 \pmod{3}$ and $p \equiv 1 \pmod{4}$, or $p \equiv 2 \pmod{3}$ and $p \equiv 3 \pmod{4}$. The first two congruences are equivalent to $p \equiv 11 \pmod{12}$, and the second two are equivalent to $p \equiv 1 \pmod{12}$.

If we want $\left( \frac{3}{p} \right) = -1$, then we want $p \equiv 1 \pmod{3}$ and $p \equiv 3 \pmod{4}$, or $p \equiv 2 \pmod{3}$ and $p \equiv 1 \pmod{4}$. For the first case, the congruence $p \equiv 1 \pmod{3}$ implies that $p \equiv 1, 4, 7, \text{ or } 10 \pmod{12}$. The congruence $p \equiv 3 \pmod{4}$ implies that $p \equiv 3, 7, \text{ or } 11 \pmod{12}$. Therefore, for both to be true, we need $p \equiv 7 \pmod{12}$.

For the second case, the congruence $p \equiv 2 \pmod{3}$ implies that $p \equiv 2, 5, 8, \text{ or } 11 \pmod{12}$ and $p \equiv 1 \pmod{4}$ implies that $p \equiv 1, 5, \text{ or } 9 \pmod{12}$.

Therefore, for both of these congruences to be true, we need $p \equiv 5 \pmod{12}$. Therefore,

$$\left( \frac{3}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv 1 \text{ or } 11 \pmod{12} \\
-1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{12}.
\end{cases}$$
We can apply Theorem 1.5, as well as the definition of the Legendre Symbol and the LQR to the following example:

Does the congruence $x^2 \equiv 631 \pmod{1093}$ have any solutions (where 631 and 1093 are both prime)?

In other terms, this is asking if 631 is a quadratic residue modulo 1093. We start by looking at the Legendre Symbol $\left(\frac{631}{1093}\right)$.

$$\left(\frac{631}{1093}\right) = \left(\frac{1093}{631}\right)$$

by the LQR, $1093 \equiv 1 \pmod{4}$ and $631 \equiv 3 \pmod{4}$

$$= \left(\frac{462}{631}\right)$$

by Theorem 1.6.1, $1093 \equiv 462 \pmod{631}$

$$= \left(\frac{14}{631}\right) \left(\frac{33}{631}\right)$$

by Theorem 1.6.2, $462 = 14 \times 33$

$$= \left(\frac{2}{631}\right) \left(\frac{7}{631}\right) \left(\frac{3}{631}\right) \left(\frac{11}{631}\right)$$

by Theorem 1.6.2, $14 = 2 \times 7, 33 = 3 \times 11$

We use Theorem 1.6.2 for $\left(\frac{2}{631}\right)$, and the LQR for the other Legendre Symbols. Since 3, 7, and 11 are all congruent to 3 modulo 4, and $631 \equiv 3 \pmod{4}$, as previously mentioned, then by the LQR, $\left(\frac{7}{631}\right) = -\left(\frac{631}{7}\right), \left(\frac{3}{631}\right) = -\left(\frac{631}{3}\right), \text{and } \left(\frac{11}{631}\right) = -\left(\frac{631}{11}\right)$.

Thus, we have

$$\left(\frac{2}{631}\right) \left(\frac{7}{631}\right) \left(\frac{3}{631}\right) \left(\frac{11}{631}\right) = (-1)^{\frac{631^2-1}{2}} \left[-\left(\frac{631}{7}\right)\right] \left[-\left(\frac{631}{3}\right)\right] \left[-\left(\frac{631}{11}\right)\right]$$

$$= (-1)^{199080} \left[-\left(\frac{1}{7}\right)\right] \left[-\left(\frac{1}{3}\right)\right] \left[-\left(\frac{1}{11}\right)\right]$$

by Theorem 1.6.1

$$= (1)(-1)(-1)(-1)$$

$$= 1$$

It is easy to see that $\left(\frac{1}{7}\right) = \left(\frac{1}{3}\right) = 1$ since 1 is always a quadratic residue, no matter the modulo, because $1^2 = 1$. We can see that $\left(\frac{4}{11}\right) = 1$ as well, since $x = 2$ is a solution to the
equation $x^2 \equiv 4 \pmod{11}$. Since $\left(\frac{631}{1093}\right) = -1$, we can conclude that 631 is not a quadratic residue modulo 1093, and thus, the equation $x^2 \equiv 631 \pmod{1093}$ does not have any solutions.

1.2 Proof of the Law of Quadratic Reciprocity

Law of Quadratic Reciprocity (LQR): If $p$ and $q$ are distinct odd primes, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv q \equiv 3 \pmod{4}$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. [1, pg. 116]

We will follow the proof from Andrews’ text. [1, pp. 121-123]

Proof: Let $\mu_1$ denote the number of integers in the set

$$\left\{q, 2q, \ldots, \frac{1}{2}(p - 1)q\right\}$$

with negative least residues modulo $p$. Let $\mu_2$ denote the number of integers in the set

$$\left\{p, 2p, \ldots, \frac{1}{2}(q - 1)p\right\}$$

with negative least residues modulo $p$. It follows from Gauss’s Lemma (since $p$ and $q$ must be prime) that $\left(\frac{p}{q}\right) = (-1)^{\mu_1}$ and $\left(\frac{q}{p}\right) = (-1)^{\mu_2}$. Then, since $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if and only if $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = 1$ we see that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if and only if

$$(-1)^{\mu_1 + \mu_2} = 1.$$ 

Thus, to prove the Law of Quadratic Reciprocity, we must show that $\mu_1 + \mu_2$ is odd if and only if $p \equiv q \equiv 3 \pmod{4}$.

From here, we proceed geometrically. We will count in two ways the lattice points (that is, points whose coordinates are integers) inside a certain hexagon. The first count will show that there are an odd number of lattice points in the hexagon if and only
if \( p \equiv q \equiv 3 \pmod{4} \). Our second count will show that there are \( \mu_1 + \mu_2 \) lattice points inside the hexagon. The two counts together will show that \( \mu_1 + \mu_2 \) is odd if and only if \( p \equiv q \equiv 3 \pmod{4} \).

**Lattice Points in proof of LQR** [1, pg. 122]

In the first quadrant of the \( xy \)-plane, we consider the hexagon \( H \) with vertices \( ABCDEF \) that lie on the rectangle \( AGDJ \) bounded by the coordinate axes and the lines \( x = p/2 \) and \( y = p/2 \), as shown above.

\( EF \) is defined by

\[
y = \frac{q}{p} x + \frac{1}{2}
\]

and \( BC \) is defined by

\[
x = \frac{p}{q} y + \frac{1}{2}
\]

The line \( BC \) has \( x \)-intercept \( \left( \frac{1}{2}, 0 \right) \), and \( EF \) has \( y \)-intercept \( \left( 0, \frac{1}{2} \right) \) and both lines are parallel to the diagonal \( AD \).
The coordinates of the points \((x, y)\) that lie in the interior of \(H\) must satisfy the inequalities

\[
0 < x < \frac{p}{2}, \quad 0 < y < \frac{q}{2},
\]

\[
y < \frac{q}{p}x + \frac{1}{2} < y > \frac{q}{p}x - \frac{q}{2p}.
\]

Note that if \((m, n)\) is any lattice point in the interior of \(H\), then so is \((\frac{p+1}{2} - m, \frac{q+1}{2} - n)\); we can verify this by substituting these coordinates into the four inequalities of (1). We now see that

\[
(m, n) = \left(\frac{p + 1}{2} - m, \frac{q + 1}{2} - n\right)
\]

if and only if \(m = \frac{p+1}{4}\) and \(n = \frac{q+1}{4}\); and \(P:\left(\frac{p+1}{4}, \frac{q+1}{4}\right)\) is a lattice point if and only if \(p \equiv q \equiv 3 \pmod{4}\). Thus the pairing of \((m, n)\) with \(\left(\frac{p+1}{2} - m, \frac{q+1}{2} - n\right)\) shows that the number of lattice points in \(H\) is odd if and only if \(p \equiv q \equiv 3 \pmod{4}\).

Now we shall consider the lattice points in \(H\) from a different point of view. It is clear that there are no lattice points on the diagonal \(y = \frac{q}{p}x\). If \((m, n)\) is a lattice point below the diagonal, then

\[
\frac{qm}{p} - \frac{q}{2p} < n < \frac{qm}{p};
\]

that is,

\[
-\frac{q}{2} < np - qm < 0
\]

(2)

We can see that in this case \(np\) has a negative least residue modulo \(q\), namely \(np - qm\).

Conversely, if \(np\) has a negative least residue, then \(np \equiv k \pmod{q}\) and \(-\frac{q}{2} < k < 0\) for some integer \(k\). Therefore, \(q|(np - k)\) by definition of congruence. Thus, \(np - k = qm\).
for some integer \( m \), or \( np - qm = k \). Thus, \( np - qm \) is a negative least residue modulo \( q \) since \( -\frac{q}{2} < k < 0 \), and we have produced an \( m \) such that (2) holds. Since \( -\frac{q}{2} < np - qm < 0 \), then \( -\frac{q}{2p} < n - \frac{qm}{p} < 0 \), and \( \frac{qm}{p} - \frac{q}{2p} < n < \frac{qm}{p} \). Therefore, \( (m, n) \) is in \( H \) and since it lies below the diagonal and above the line \( y = \frac{q}{p}x + \frac{1}{2} \). Thus, since \( \mu_2 \) is the number of integers in the set \( \{ p, 2p, \ldots, \frac{1}{2}(q - 1)p \} \) with negative least residues modulo \( q \), there are \( \mu_2 \) lattice points in \( H \) below the diagonal \( AD \).

Similarly, we find \( \mu_1 \) lattice points in \( H \) above the main diagonal.

We conclude that \( \mu_1 + \mu_2 \) (the total number of lattice points in \( H \)) is odd if and only if \( p \equiv q \equiv 3 \pmod{4} \); thus, the Law of Quadratic Reciprocity is proved. ■

[1, pp. 121-123]


Section 2: Cryptography

Cryptography has been around for millennia. It has always been focused on one basic problem, that of providing secret communications. Modern cryptography, in particular, is interested in all tasks that involve secret agents, human or otherwise, that wish to obtain or share some information while still preserving the secrecy of other information. The general goal of cryptography is to construct schemes, called protocols, which maintain a desired functionality (privacy requirements, rules, etc.), even when faced with malicious attempts to hinder this functionality. Therefore, an important aspect of cryptography besides privacy is resilience: one would like privacy to be guaranteed even if one is not certain that the other participants are behaving honestly. There are two key assumptions underlying most cryptosystems. First, it is assumed that all parties involved, including the malicious adversaries, are computationally limited. That is, we assume that there is a point at which our encryption would be too difficult to crack. Second, it is assumed that the cryptosystems involve difficult functions and are therefore unable to be easily cracked. This is important because the point of cryptography is not just to have secrets, but to actually be able to use them without giving away information. [2, pg. 601]

Symmetric encryption algorithms like Triple DES and AES use the same key both to encrypt and decrypt. When used correctly, these systems can provide virtually unbreakable security for the information that they are used to protect. It is difficult, however, to securely distribute a symmetric key to both the sender and the recipient of an encrypted message. These difficulties, though, do not stop the symmetric encryption schemes from being widely used in such technology as ATM machines and checkouts.
ATMs and checkouts use symmetric encryption so successfully because they only communicate with a single well-known system. Unfortunately, very few businesses are this simple; therefore, systems have to become more complex. In more complex systems, users each need a different key to be able to communicate securely with other users, or else users would be able to decrypt messages that were not intended for them. Having a large number of users would also give us a large number of keys that we may need to securely update on a regular basis. Public-key cryptography was invented to try to solve this symmetric key distribution problem. [5]

2.1 Public Key Cryptography

In a public-key system, each person gets a pair of keys, one known as the public key and the other known as the private key. The two keys are mathematically related so that information that is encrypted with the public key can only be decrypted with the corresponding private key and vice versa. Therefore, if the public key is made available to everyone but the private key is kept secret, then anyone can encrypt a message to someone by using their public key, but only the intended recipient can decrypt the message by using their corresponding private key. [5]

A simple example of public-key cryptography can be seen in the following diagram:
We start with two users, Bob and Alice. If Bob wants to send the message “Hello Alice!” to Alice, he uses Alice’s public key to encrypt the message. He then sends the encrypted message to Alice and she uses her corresponding private key to decrypt the message.

The original idea of using public keys assumed that the keys would be easily accessible in a public directory of some sort, similar to a universal phone book, but a practical implementation of this idea has evaded technologists for nearly 30 years.

Another problem that makes the use of public-key technology difficult is key recovery. Recovery of a private key is often required, for example, when the original recipient of the encrypted message is not available, but you still need to decrypt the message. In this case, you would need to somehow access the same private key that the recipient of the message has, but because private keys are usually randomly generated, the only way to do this is to securely archive copies of all of the private keys. This leads to many problems, such as significant cost and complexity of ensuring that backups are complete and recovery plans are comprehensive, in addition to the cost of the groundwork needed to achieve this. [5]
A famous example of a public-key encryption scheme is RSA. In the RSA scheme, if a user, say Alice, wants to receive messages, she publishes a large composite number \( N \), called a public key, which is a product of two large primes \( P \) and \( Q \), which are part of Alice’s private key. If one knows \( N \), then one can encrypt any message, but to decrypt it, one would need to know \( P \) and \( Q \). Therefore, if factorization of \( N \) is difficult, then only Alice would be able to decrypt messages. [2, pg. 602]

### 2.2 Identity-Based Encryption

Identity-based encryption (IBE) is a form of public-key cryptography that allows you to calculate a public key directly from a user’s identity, for example, his email address. Adi Shamir first introduced the idea of IBE in 1984, as a way to try to eliminate difficulties associated with using a public-key system, such as key recovery. His idea was to create a way of calculating a public key from a user’s identity, and he described such a system in the following way:

An identity-based scheme resembles an ideal mail system: If you know somebody’s name and address you can send him messages that only he can read, and you can verify the signatures that only he could have produced. It makes the cryptographic aspects of the communication almost transparent to the user, and it can be used effectively even by laymen who know nothing about keys or protocols. [5]

The form of identity used to calculate an IBE key depends on the application. For encrypting emails, a string that represents the e-mail address of the recipient might be a good choice, but in other applications, a phone number, a device serial number, or an IP
address might be more logical. Essentially, any identity that is globally unique can be used. [5]

The general architecture of any complete IBE scheme is the same. In each case, the sender calculates the public key of the recipient and then the recipient has to authenticate his/herself to a private key generator (PKG) or server to obtain the corresponding private key. Therefore, for Alice to send an encrypted message to Bob, she will first calculate Bob's public key and then use this public key to encrypt the message. After Bob receives the encrypted message, he then authenticates himself to a PKG, which will then securely send the corresponding private key to him. He can then use the private key to decrypt the message and view its contents. [5] This general architecture is illustrated in the following diagram:

Since IBE is a public-key technology, it has all the benefits that other public-key technologies have, but it also brings other benefits, since IBE keys are calculated instead of being randomly generated. Therefore, there is no requirement for looking up public
keys, and thus, one of the big practical difficulties that has been associated with public-key cryptography is no longer an issue. Also, since we calculate a user’s private key when he initially requests it, we can easily recalculate it at any other time, giving us built-in key recovery, which is essential for an encryption scheme to have if it is going to be used by businesses. A useful consequence of built-in key recovery is that it is easy to integrate message hygiene technologies, which make it feasible to actually scan encrypted messages for malicious content like viruses, spam, or phishing attacks. [5]
Section 3: Cocks IBE Scheme

The Cocks IBE Scheme is a cryptosystem that allows identity-based encryption and is based on the difficulty of the composite quadratic residue problem, which has to do with when a number is a square modulo a positive integer $n$. This system has an authority that generates a public modulus $M$ that is universally available. This modulus is the product of two primes $P$ and $Q$, held privately by the authority, where $P$ and $Q$ are both congruent to 3 mod 4. Although $M$ is public, $P$ and $Q$ are large primes, so factorization of $M$ is very difficult.

The system also makes use of a universally available secure hash function. Hash functions are often called "one-way" functions. That is, if we have $x$, then it is easy to find $f(x)$; however, if we have $f(x)$, it is hard to calculate $x$. The scheme uses this hash function to shorten the user's identity to a smaller, more manageable number. Then, if a user, say Alice, wishes to register in order to be able to receive encrypted data, she presents her identity (e.g. e-mail address) to the authority. In return, she is given a private key with properties described below. If a user Bob wishes to send encrypted data to Alice, he will be able to do this knowing only Alice's public identity, e.g. her email address, and the universal system parameters, such as $M$. This eliminates the need for a public key directory. [3]

3.1 Set-up

When Alice presents her identity to the authority, the hash function is applied to the string representing her identity to produce a value $a$ modulo $M$ such that the Jacobi symbol $\left(\frac{a}{M}\right)$ is +1. This is a public process that anyone holding the universal parameters
and knowing Alice’s identity can replicate. This will typically involve multiple applications of the hash function in a systematic way to produce a set of candidate values for a, stopping when \( \left( \frac{a}{M} \right) = +1 \). This value of a is fixed for each message. [3]

It is useful to note that the Jacobi symbol can be calculated without knowledge of the factorization of M. For example, if we are trying to calculate the Jacobi symbol \( \left( \frac{13}{77} \right) \), we know from the Law of Quadratic Reciprocity that

\[
\left( \frac{13}{77} \right) = \left( \frac{77}{13} \right) = (-1)^{\frac{(13-1)(77-1)}{4}}
\]

\[
\left( \frac{13}{77} \right) = (-1)^{\frac{(12)(76)}{4}} \left( \frac{77}{13} \right)^{1}
\]

\[
= (-1)^{228} \left( \frac{77}{13} \right)
\]

\[
= \left( \frac{12}{13} \right)
\]

\[
= \left( \frac{4}{13} \right) \left( \frac{3}{13} \right)
\]

\[
= \left( \frac{3}{13} \right) \left( \frac{13}{3} \right) = \left( \frac{1}{3} \right) = 1
\]

We can see that \( \left( \frac{77}{13} \right) = \left( \frac{12}{13} \right) \) since 77 \( \equiv \) 12 (mod 13) and \( \left( \frac{4}{13} \right) = 1 \) since 4 is a quadratic residue modulo 13, since \( 2^2 = 4 \equiv 4 \) (mod 13). Also, \( \left( \frac{3}{13} \right) = \left( \frac{13}{3} \right) = \left( \frac{1}{3} \right) \) using the Law of Quadratic Reciprocity and the fact that 13 \( \equiv \) 1 (mod 3). It is then easy to see that 1 is a quadratic residue modulo 3 and thus \( \left( \frac{1}{3} \right) = 1 \).

More generally, we can see that this method will work for any \( \left( \frac{a}{M} \right) \). We know that M will always be odd, since it is the product of two large primes P and Q and all primes greater than two are odd. If a is odd, then the above method works in general by
the Law of Quadratic Reciprocity. If \( a \) is even, then we can split \( \left( \frac{a}{M} \right) \) into its odd and even parts, using the same steps as above for the odd part, and using Theorems 1.5 and 1.9 to calculate the even part. Therefore, we can use the above method to calculate the Jacobi symbol using theorems we already know, and without knowledge of the factorization of \( M \).

Therefore, as \( \left( \frac{a}{M} \right) = \left( \frac{a}{P} \right) \left( \frac{a}{Q} \right) = +1, \left( \frac{a}{P} \right) = \left( \frac{a}{Q} \right), \) and \( \left( \frac{a}{P} \right) \) and \( \left( \frac{a}{Q} \right) \) are both either +1 or −1. If \( \left( \frac{a}{P} \right) \) and \( \left( \frac{a}{Q} \right) \) are both +1, then \( a \) is a square modulo both \( P \) and \( Q \), and hence is a square modulo \( M \). If \( \left( \frac{a}{P} \right) \) and \( \left( \frac{a}{Q} \right) \) are both −1, then \( -a \) is a square modulo \( P, Q \) and hence \( M \). The latter case comes about because by construction \( P \) and \( Q \) are both congruent to 3 mod 4, and so \( \left( \frac{-1}{P} \right) = \left( \frac{-1}{Q} \right) = -1 \). [3] We can see this since if \( P \equiv 3 \mod 4 \), then \( P = 3 + 4k \) for some positive integer \( k \), by the definition of congruence, and thus by Theorem 1.10,

\[
\left( \frac{-1}{P} \right) = (-1)^{P-1 \over 2} = (-1)^{3+4k-1 \over 2} = (-1)^{2+2k \over 2} = (-1)^{1+2k}
\]

The value \( 1+2k \) will always yield an odd number and −1 to an odd power equals −1. Therefore, \( \left( \frac{-1}{P} \right) = (-1)^{1+2k} = -1 \) whenever \( P \) is congruent to 3 mod 4. Similarly,

\[
\left( \frac{-1}{Q} \right) = -1 \text{ whenever } Q \text{ is congruent to 3 mod 4. Therefore, } \left( \frac{-1}{P} \right) = \left( \frac{-1}{Q} \right) = -1.
\]

Thus, if \( \left( \frac{a}{P} \right) \) and \( \left( \frac{a}{Q} \right) \) are both −1, then

\[
\left( \frac{-a}{P} \right) = \left( \frac{-1}{P} \right) \left( \frac{a}{P} \right) = (-1)(-1) = 1
\]

and

33
\[
\left( \frac{-a}{Q} \right) = \left( \frac{-1}{Q} \right) \left( \frac{a}{Q} \right) = (-1)(-1) = 1,
\]

and thus, \(-a\) is a quadratic residue modulo both \(P\) and \(Q\).

Therefore either \(a\) or \(-a\) will be a quadratic residue modulo both \(P\) and \(Q\), and therefore modulo \(M\). The authority is the only one who can calculate the square root modulo \(M\), and he presents such a root to Alice. We shall call this value \(r\). The authority determines such a root by calculating

\[
r \equiv a \frac{M+5-(P+Q)}{8} \pmod{M}
\]

Such an \(r\) satisfies either \(r^2 \equiv a \pmod{M}\) or \(r^2 \equiv -a \pmod{M}\) depending on which of \(a\) or \(-a\) is a square modulo \(M\). [3]

**THEOREM:** For \(r = a \frac{M+5-(P+Q)}{8} \pmod{M}\), \(r^2 \equiv \pm a \pmod{M}\) whenever \(M = PxQ\), where \(P, Q\) are both congruent to 3 modulo 4.

**PROOF:** Since \(r\) is defined as \(a \frac{M+5-(P+Q)}{8} \pmod{M}\), then

\[
r^2 = \left( a \frac{M+5-(P+Q)}{8} \right)^2 \pmod{M}
\]

\[
= \left( a \frac{PQ+5-(P+Q)}{8} \right)^2 \pmod{M}
\]

\[
= \left( a \frac{PQ-P-Q+1+4}{8} \right)^2 \pmod{M}
\]

\[
= \left( a \frac{\phi(PQ)+4}{8} \right)^2 \pmod{M}
\]

\[
= a \frac{\phi(PQ)+4}{4} \pmod{M}
\]

\[
= a \frac{\phi(PQ)}{4} + 1 \pmod{M}
\]

\[
= a \frac{\phi(PQ)}{4} \cdot a \pmod{M}
\]

34
We can see that 
\[
\left( a^{\frac{P-1-P-Q+1+4}{2}} \right)^2 = \left( a^{\frac{\phi(PQ)+4}{8}} \right)^2 \mod M \text{ since } \phi(PQ) = (P-1)(Q-1) = PQ - P - Q + 1.
\]
We now want to show that \( a^{\frac{\phi(PQ)}{4}} \equiv \pm 1 \mod M \). This is equivalent to showing that \( a^{\frac{(P-1)(Q-1)}{4}} \equiv \pm 1 \mod PQ \), since \( M = P \times Q \), as previously defined, and \( \phi(PQ) = (P - 1)(Q - 1) \). As stated previously, as \( \left( \frac{a}{M} \right) = +1, \left( \frac{a}{P} \right) = \left( \frac{a}{Q} \right) \).

There are two cases here for the values of \( \left( \frac{a}{P} \right) \) and \( \left( \frac{a}{Q} \right) \); either both will equal 1 or both will equal -1.

**Case 1:** Let \( \left( \frac{a}{P} \right) = \left( \frac{a}{Q} \right) = 1 \). Then \( a \) is a square or quadratic residue both mod \( P \) and mod \( Q \). Therefore, by Euler's Criterion,
\[
\frac{P-1}{a^{2}} \equiv 1 \mod P \quad \text{and} \quad \frac{Q-1}{a^{2}} \equiv 1 \mod Q.
\]
Then, raising both sides of the first equation to the power \( \frac{Q-1}{2} \) and both sides of the second equation to the power \( \frac{P-1}{2} \), we find that
\[
\frac{a^{(P-1)(Q-1)}}{4} \equiv 1 \mod P
\]
and
\[
\frac{a^{(P-1)(Q-1)}}{4} \equiv 1 \mod Q
\]
since 1 raised to any power always gives back 1. Therefore, \( P \left( a^{\frac{(P-1)(Q-1)}{4}} - 1 \right) \) and \( Q \left( a^{\frac{(P-1)(Q-1)}{4}} - 1 \right) \). Therefore, by Theorem 1.1, \( PQ \left( a^{\frac{(P-1)(Q-1)}{4}} - 1 \right) \), and thus
\[
a^{\frac{\phi(PQ)}{4}} \equiv +1 \mod M.
\]
Case 2: Let \((\frac{a}{P}) = \frac{a}{Q} = -1\). Then, as shown above on pg. 31, \(-a\) is a square or quadratic residue both mod \(P\) and mod \(Q\). Thus, similarly to Case 1,

\[
(-a) \frac{(P-1)(Q-1)}{4} \equiv 1 \mod P
\]

and

\[
(-a) \frac{(P-1)(Q-1)}{4} \equiv 1 \mod Q.
\]

Therefore,

\[
(-1) \frac{(P-1)(Q-1)}{4} (a) \frac{(P-1)(Q-1)}{4} \equiv 1 \mod P
\]

and

\[
(-1) \frac{(P-1)(Q-1)}{4} (a) \frac{(P-1)(Q-1)}{4} \equiv 1 \mod Q.
\]

Since \(P \equiv Q \equiv 3 \mod 4\), then \(P = 3 + 4k\) and \(Q = 3 + 4l\) for some positive integers \(k\) and \(l\) by the definition of congruence. Therefore,

\[
(-1) \frac{(P-1)(Q-1)}{4} = (-1)^{\frac{(3+4k-1)(3+4l-1)}{4}}
\]

\[
= (-1)^{\frac{(2+4k)(2+4l)}{4}}
\]

\[
= (-1)^{\frac{(4+8k+8l+16kl)}{4}}
\]

\[
= (-1)^{1+2(k+l)+4kl}
\]

The value \(1 + 2(k + l) + 4kl\) will always yield an odd number and \(-1\) to an odd power equals \(-1\). Therefore, \((-1)^{\frac{(P-1)(Q-1)}{4}} = (-1)^{1+2(k+l)+4kl} = -1\) whenever \(P\) and \(Q\) are both congruent to \(3 \mod 4\). Therefore,

\[
(-1) \frac{(P-1)(Q-1)}{4} (a) \frac{(P-1)(Q-1)}{4} \equiv - (a) \frac{(P-1)(Q-1)}{4} \equiv 1 \mod P
\]

and
Thus, multiplying both sides of both congruences by $-1$, we see that
\[
\alpha \frac{(P-1)(Q-1)}{4} \equiv -1 \mod P
\]
and
\[
\alpha \frac{(P-1)(Q-1)}{4} \equiv -1 \mod Q
\]
Therefore, $P \mid \left( \alpha \frac{(P-1)(Q-1)}{4} + 1 \right)$ and $Q \mid \left( \alpha \frac{(P-1)(Q-1)}{4} + 1 \right)$. Then, by Theorem 1.1, $PQ \mid \left( \alpha \frac{(P-1)(Q-1)}{4} + 1 \right)$, and thus $\alpha \frac{\phi(PQ)}{4} \equiv -1 \mod M$.

Therefore, $\alpha \frac{\phi(PQ)}{4} \equiv \pm 1 \mod M$. Thus, $r^2 = \alpha \frac{\phi(PQ)}{4} \cdot \alpha \mod M \equiv \pm \alpha \mod M$. \[\square\]

In what follows, we will assume without loss of generality that $r^2 \equiv a \pmod{M}$.

Users wishing to send encrypted data to Alice who do not know whether she has received a root of $a$ or a root of $-a$ will need to double up the amount of keying data they send as described later. In general, it is not true that exactly one of $a$ or $-a$ will be squares modulo $M$ and this is one of the main reasons we use $P$ and $Q$ both congruent to 3 modulo 4. [3]

### 3.2 Encryption

Assume we have two users, Alice and Bob. If Bob wants to send an encrypted message to Alice, he encrypts the data using symmetric encryption. He then sends to Alice each bit of the message in turn as follows:

Let $x$ be a single bit of the message, coded as $+1$ or $-1$. That is, 0’s are converted to $-1$’s.
Bob then chooses a value $t$ at random modulo $M$, such that the Jacobi symbol 

$$\left( \frac{t}{M} \right) = x.$$ 

Then he sends $s = (t + at^{-1}) \pmod{M}$ to Alice.

Alice can only see the value of $s$, whereas Bob can see the value of $s$ and how it was calculated since he knows $t$. Both Alice and Bob know the value of $a$, as it is part of Alice's public key. [3]

### 3.3 Decryption

Alice recovers the bit $x$ by computing $\left( \frac{s + 2r}{M} \right)$. This works because

$$s + 2r = (t + at^{-1}) + 2r \mod M \quad \text{since } s = (t + at^{-1}) \pmod{M}, \text{as defined above}$$

$$= t + 2r + r^2 t^{-2} \mod M \quad \text{since } r^2 \equiv a \pmod{M}$$

$$= t(1 + rt^{-1})^2 \mod M$$

It follows that the Jacobi symbol $\left( \frac{s + 2r}{M} \right) = \left( \frac{t(1 + rt^{-1})^2}{M} \right) = \left( \frac{t}{M} \right) \left( \frac{1 + rt^{-1}}{M} \right)^2$. The Jacobi Symbol $\left( \frac{1 + rt^{-1}}{M} \right)^2 = 1$ since $(1 + rt^{-1})$ is a square; that is, we can find a solution to the equation $y^2 \equiv (1 + rt^{-1})^2 \pmod{M}$, namely $y = 1 + rt^{-1}$. Thus, $\left( \frac{t}{M} \right) \left( \frac{1 + rt^{-1}}{M} \right)^2 = \left( \frac{t}{M} \right) = x$. [3]

### 3.4 Problems

If Bob does not know whether $a$ or $-a$ is the square for which Alice holds the root, then he will have to replicate the encryption steps above, using different randomly chosen $t$ values to send the same $x$ bits as before, and transmitting $s = (t - at^{-1}) \pmod{M}$
\( M \) to Alice at each step. This then doubles the amount of keying data that Bob must send. It would be useful if we could find a way to avoid having to send this extra information, but at present this is an unsolved problem. [3]

Computationally, this system is not too expensive. If the transport key is \( L \) bits long, then Bob’s work consists of needing to compute \( L \) Jacobi symbols and \( L \) divisions mod \( M \). Alice’s work consists mainly of computing \( L \) Jacobi symbols. Depending on the implementation and for typical parameter values (e.g. \( L = 128 \) and \( M \) of size 1024 bits), this is likely to be no more work than what is needed for a single exponentiation modulo \( M \). The main issue regarding practicality is the bandwidth requirement, since each bit of the transport key requires a number of size up to \( M \) to be sent. If we have a 128 bit transport key, and are using a 1024 bit modulus \( M \), Bob will need to send 16K bytes of keying material. If he does not know whether Alice has received the square root of \( a \) or of \(-a\), then he will have to double this. [2] This much overhead may seem impractical for encrypting routine business communications, but it is likely less of a concern if we use the scheme for exchanging keying material that only needs to be done infrequently. This specific feature of the Cocks IBE scheme has prevented it from gaining widespread acceptance. [5]

3.5 Security

Clearly, one way to break the scheme is to factor \( M \). This is a weak link, so shared knowledge methods of generating \( M \) and the use of multiple authorities will be desirable. With this shared generation of \( M \), it is also feasible to generate the exponent
that is used to compute square roots in a shared fashion, so that no master secret ever has to exist in a single location. [3]

We study the security of this scheme with the assumption that \( M \) has not been factored. We will also assume that Bob has had to double his keying information and sends the pair \((y_1, y_2)\), where \( y_1 \equiv (t_1 + at_1^{-1}) \pmod{M} \) and \( y_2 \equiv (t_2 - at_2^{-1}) \pmod{M} \) to Alice.

3.5.1 Security Proof

**Theorem:** Let \( y_1 \equiv (t_1 + at_1^{-1}) \pmod{M} \) and \( y_2 \equiv (t_2 - at_2^{-1}) \pmod{M} \). Given \( y_1, y_2 \) provides no information about \( x = \left( \frac{t_1}{M} \right) \), and vice versa; that is, given \( y_2, y_1 \) provides no information about \( x = \left( \frac{t_2}{M} \right) \) [7]

**Proof:** Suppose that \( y = y_2 \). Then \( y \equiv (t_2 - at_2^{-1}) \pmod{M} \) and \( y^2 \equiv a \pmod{M} \).

We also know that \( y_2 \equiv (t_2 - at_2^{-1}) \pmod{M} \). Then, multiplying \( y_2 \equiv t_2 - at_2^{-1} \pmod{M} \) by \( t_2 \) on both sides and rearranging, we get

\[
\frac{t_2^2}{M} - y_2 t_2 - a \equiv 0 \pmod{M}
\]

Therefore,

\[
t^2 - y_2 t_2 - a \equiv 0 \pmod{P} \quad (1) \text{ and }
\]

\[
t^2 - y_2 t_2 - a \equiv 0 \pmod{Q} \quad (2)
\]

Equations (1) and (2) are quadratic equations modulo a prime; therefore they each have exactly two solutions. Let \( t_{p_1}, t_{p_2} \) be the roots of equation (1), and \( t_{q_1}, t_{q_2} \) be the roots of equation (2). Therefore, by the Chinese Remainder Theorem, there will be four possible values of \( t_2 \) and
\((t_2 - t_{p_1})(t_2 - t_{p_2}) \equiv 0 \pmod{P}\) \hspace{1cm} (3)

and \((t_2 - t_{q_1})(t_2 - t_{q_2}) \equiv 0 \pmod{Q}\). \hspace{1cm} (4)

Therefore,

\[ t_2^2 - (t_{p_1} + t_{p_2})t_2 + t_{p_1} \cdot t_{p_2} \equiv t_2^2 - y_2 t_2 - a \pmod{P} \]

and \[ t_2^2 - (t_{q_1} + t_{q_2})t_2 + t_{q_1} \cdot t_{q_2} \equiv t_2^2 - y_2 t_2 - a \pmod{Q} \]

since (1) and (3) are congruent to 0 modulo \(P\) and (2) and (4) are congruent to 0 modulo \(Q\). Thus,

\[ t_{p_1} \cdot t_{p_2} \equiv -a \pmod{P} \]

\[ t_{q_1} \cdot t_{q_2} \equiv -a \pmod{Q} \]

then

\[ \left( \frac{t_{p_1} \cdot t_{p_2}}{P} \right) \equiv \left( \frac{-a}{P} \right) \equiv -1 \equiv \left( \frac{t_{p_1}}{P} \right) \left( \frac{t_{p_2}}{P} \right) \]

\[ \left( \frac{t_{q_1} \cdot t_{q_2}}{Q} \right) \equiv \left( \frac{-a}{Q} \right) \equiv -1 \equiv \left( \frac{t_{q_1}}{Q} \right) \left( \frac{t_{q_2}}{Q} \right) \]

Therefore for \(t_{p_1}\) and \(t_{p_2}\), either \(\left( \frac{t_{p_1}}{P} \right)\) or \(\left( \frac{t_{p_2}}{P} \right)\) equals -1 and the other equals +1. The same is true for \(t_{q_1}\) and \(t_{q_2}\). Thus, since \(t_{p_1}, t_{p_2}, t_{q_1}, t_{q_2}\) are the possible values of \(t_2\),

\[ x = \left( \frac{t_2}{M} \right) \text{ has a } \frac{1}{4} \text{ possibility of equaling } +1 \text{ and a } \frac{1}{4} \text{ possibility of equaling } -1. \]

Therefore, we have no information about \(x\) because there is an equal likelihood of \(x\).
equaling +1 or -1. In order to get this information, we would need to have a procedure that can distinguish the two cases of \( \left( \frac{a}{M} \right) = +1 \); that is, we would need to determine somehow whether \( a \) is a square or \( -a \) is a square without factoring \( M \). This is the composite quadratic residue problem, which is currently unsolved.

An attacker would be, in practice, presented with a set of many such terms \((t + at^{-1}) \mod M\) and possibly also \((t - at^{-1}) \mod M\) for different values of \( t \). Therefore, we want values of \( t \) that are independent and randomly distributed over the set of values with the desired key value.

### 3.6 Example

To better understand the Cocks IBE Scheme, we will look at an example with \( P \) and \( Q \) both very small primes. We let \( P = 11 \) and \( Q = 7 \); therefore, \( M = P \times Q = 77 \).

Suppose that Bob wants to send the message “HI” to Alice. We first convert the message to ASCII and find that HI = [104, 105]. We then convert these numbers to binary to get [1101000, 1101001]. According to the encryption rules of the scheme, we want to have a string of 1’s and -1’s; therefore we convert all 0’s to -1’s, giving us \([(1, 1, -1, 1, -1, -1, -1), (1, 1, -1, 1, -1, -1, 1)]\). To encrypt the entire message, we would then apply the encryption steps to each bit of this string. For this example, we will go through the encryption and decryption steps just for the first bit.

To set the scheme up in general, Alice would present her identity and then the hash function would be applied to the string representing her identity to produce a value \( a \) modulo \( M \) such that the Jacobi symbol \( \left( \frac{a}{M} \right) \) is +1. For this example, we will simply let \( a \) be the number of letters in the user’s name. Suppose I, Shannon Prager, am the user in
this case. Then \( a = 13 \) and \( \left( \frac{13}{77} \right) = +1 \). We then determine the square root, \( r \), of \( a \), by calculating

\[
r = a^{\frac{M+S-(P+Q)}{8} \mod M}
\]

\[
= 13^{\frac{77+S-(11+7)}{8} \mod 77}
\]

\[
= 13^8 \mod 77
\]

\[
\equiv 36 \mod 77
\]

We can see that \( 36^2 = 1296 \equiv -13 \mod 77 \), therefore \( r^2 \equiv -a \mod 77 \), and hence, \(-a\) is a square modulo 77.

Now to encrypt the first bit, \( x = 1 \), we must choose a random \( t \) such that \( \left( \frac{t}{77} \right) = x \). We let \( t = 9 \) since the Jacobi symbol \( \left( \frac{9}{77} \right) = 1 \). If Bob does not know whether \( a \) or \(-a\) is the square for which I hold the root, then Bob will have to send both \( s_1 = (t + at^{-1}) \mod M \) and \( s_2 = (t - at^{-1}) \mod M \) to me. Calculating both of these, we find that

\[
s_1 = (9 + 13 \cdot 9^{-1}) \mod 77
\]

\[
= (9 + 13 \cdot 60) \mod 77
\]

\[
= 789 \mod 77
\]

\[
\equiv 19 \mod 77
\]

and

\[
s_2 = (9 - 13 \cdot 9^{-1}) \mod 77
\]

\[
= (9 - 13 \cdot 60) \mod 77
\]

\[
= -771 \mod 77
\]

\[
\equiv 76 \mod 77
\]
It is useful to note that \( s_1 = 19 \) is the case where \( a \) is a square modulo 77, and \( s_2 = 76 \) is the case where \(-a\) is a root modulo 77. Bob then sends the pair \((s_1, s_2) = (19, 76)\) to me.

I receive this pair and compute the Jacobi symbols \( \left( \frac{s_1 + 2r}{M} \right) \) and \( \left( \frac{s_2 + 2r}{M} \right) \):

\[
\left( \frac{s_1 + 2r}{M} \right) = \left( \frac{19 + 2 \cdot 36}{77} \right) = \left( \frac{91}{77} \right) = 0 \neq x
\]

\[
\left( \frac{s_2 + 2r}{M} \right) = \left( \frac{76 + 2 \cdot 36}{77} \right) = \left( \frac{148}{77} \right) = 1 = x
\]

We can see that we do not get back \( x \) when computing the Jacobi symbol with \( s_1 \). This is due to the fact that \( s_1 \) is for the case where \( r^2 \equiv a \mod 77 \), but for this example, it was shown that we are in the case where \( r^2 \equiv -a \mod 77 \). Therefore, we get \( x \) back when computing the Jacobi symbol with \( s_2 \) since this is the case where \( r^2 \equiv -a \mod 77 \).

To encrypt the entire message, Bob would need to go through and encrypt the rest of the bits, using a different randomly chosen \( t \) value to encrypt each bit. Also, if Bob does not know whether \( a \) or \(-a\) is the square for which I hold the root, then he will have to double the amount of keying information he sends, sending both \( s_1 \) and \( s_2 \) to me.

In general, if Bob sends both \( s_1 \) and \( s_2 \), he must note which goes with \( a \) being a square and which goes with \(-a\) being a square. Since Alice knows \( r \) and \( a \), she can compute \( r^2 \) and see if she gets \( a \) or \(-a\).
Conclusion

The Cocks IBE Scheme is a very secure cryptosystem. The only public parameters of the system are the square $a$ and the modulus $M$. We have shown that knowing any information about the Jacobi symbol $\left(\frac{e}{M}\right)$ would be equivalent to solving the composite residue problem, or finding an $x$ such that $x^2 \equiv a \mod M$, which is currently unsolved. If factorization of $M$ is known, then $x^2 \equiv a \mod M$ can be broken up into congruences involving $P$ and $Q$ and these can be solved using known theorems. However, $P$ and $Q$ are chosen to be very large primes, so factorization of $M$ is extremely difficult.

The main issue regarding the practicality of the Cocks IBE Scheme is the bandwidth requirement, since each bit of the transport key requires a number of size up to $M$ to be sent. If Bob does not know whether Alice has received the square root of $a$ or of $-a$, then he will have to double the amount of keying data he must send. This specific feature of the Cocks IBE Scheme has prevented it from gaining widespread acceptance.
References


