Application of the Chinese Remainder Theorem to Cryptography and Cybersecurity

Michael Khalfin
Plainview Old-Bethpage JFK High School
Grade 11
March 5, 2021

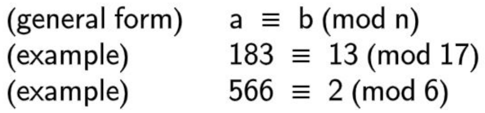
ABSTRACT

We introduce modular arithmetic and properties of congruences. Then we show how to solve a linear congruence equation, using intuition and by applying the Extended Euclidean Algorithm. Building on this concept, we introduce linear congruence systems, which we solve by the Chinese Remainder Theorem. Additionally, we briefly review the practice of cryptography, before exploring one method called RSA encryption in detail. RSA cryptosystems rely on modular exponentiation, which we demonstrate through a banker-client model example. Finally, we implement a new concept where we can combine cryptosystems to create networks involving unique exchanges. This is a novel idea that can be used to generate data for scientific induction and share secrets among various parties.

BACKGROUND

a. Modular arithmetic

Modular arithmetic is a subset of number theory where the focus is on working with integer remainders.[1] This is achieved through implementation of **linear congruences**, where integers a and b are congruent modulo n if their remainders when divided by n are the same.



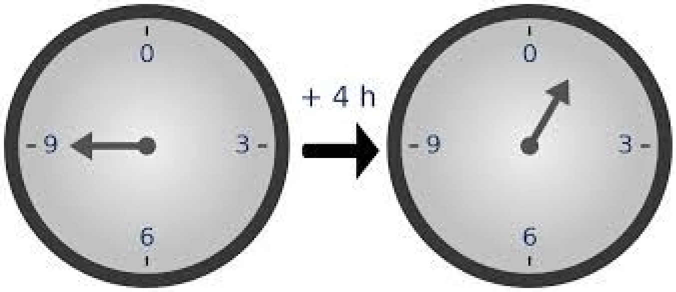
(general form) $a \equiv b \pmod{n}$

(example) $183 \equiv 13 \pmod{17}$

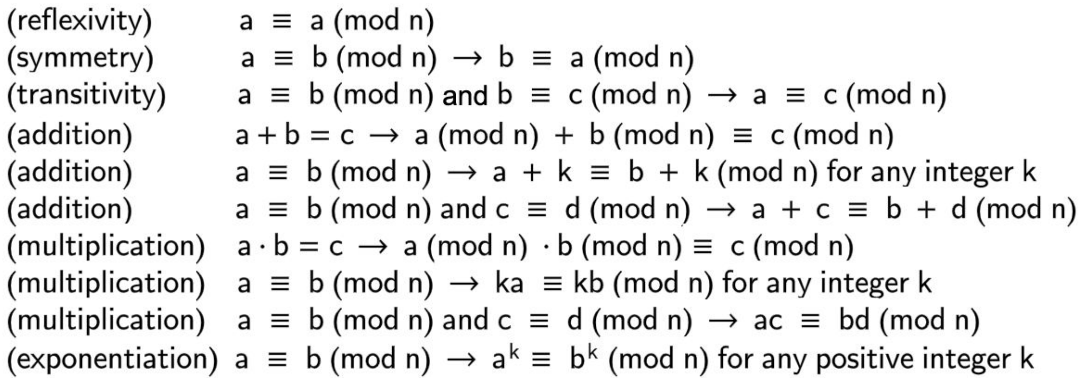
(example) $566 \equiv 2 \pmod{6}$

Figure 1. Linear Congruences.

Think of linear congruences as wrapping a number around a circle. The circle has equally sized increments which include all integers from 0 to n - 1. Move around the clock a steps and the number that we land on is the residue, or remainder, modulo n. If b has the same result modulo n then a and b are congruent modulo n.



We will not take the time to prove it here, but linear congruences have several key properties that can be manipulated.[1, 2]



(reflexivity)	$a \equiv a \pmod{n}$
(symmetry)	$a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$
(transitivity)	$a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \rightarrow a \equiv c \pmod{n}$
(addition)	$a + b = c \rightarrow a \pmod{n} + b \pmod{n} \equiv c \pmod{n}$
(addition)	$a \equiv b \pmod{n} \rightarrow a + k \equiv b + k \pmod{n}$ for any integer k
(addition)	$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n} \rightarrow a + c \equiv b + d \pmod{n}$
(multiplication)	$a \cdot b = c \rightarrow a \pmod{n} \cdot b \pmod{n} \equiv c \pmod{n}$
(multiplication)	$a \equiv b \pmod{n} \rightarrow ka \equiv kb \pmod{n}$ for any integer k
(multiplication)	$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n} \rightarrow ac \equiv bd \pmod{n}$
(exponentiation)	$a \equiv b \pmod{n} \rightarrow a^k \equiv b^k \pmod{n}$ for any positive integer k

Figure 2. Properties of Linear Congruences.

The properties from Figure 2 will be our toolbox for working with linear congruences. Reflexivity, symmetry, and transitivity are 3 properties which apply to every **equivalence relation**. In an equivalence relation, equivalence classes are ways of grouping numbers according to an algorithm. Modulus is an equivalence relation where the algorithm is the remainder of an integer division expression.

Sometimes, linear congruences will be similar to algebraic equations. This is when they will include a variable that needs to be solved for. Take the linear congruence

$$5x \equiv 3 \pmod{7}$$

The minimal solution x is x = 2. We can use our intuition to solve simple linear congruences the same way we would approach an easy algebraic equation like 3x = 12 - x where x = 3. That being said, it is not always feasible to solve linear congruence problems by inspection. When this happens, we turn to the **Extended Euclidean Algorithm**, a concept in number theory which has been used for thousands of years.

Essentially, we use the algorithm to solve for the **multiplicative inverse** of the modulo n. Then we can manipulate our congruence equation to get the value for x. Integer b is the multiplicative inverse of a number modulo n if

$$ab \equiv 1 \pmod{n}$$

The steps for the Extended Euclidean Algorithm are shown in Figure 3.

$$\begin{array}{lll}
q_1 = \left\lfloor \frac{a}{b} \right\rfloor & a = b\, q_1 + r_1 & r_1 = a - b\, q_1 \\
q_2 = \left\lfloor \frac{b}{r_1} \right\rfloor & b = q_2\, r_1 + r_2 & r_2 = b - q_2\, r_1 \\
q_3 = \left\lfloor \frac{r_1}{r_2} \right\rfloor & r_1 = q_3\, r_2 + r_3 & r_3 = r_1 - q_3\, r_2 \\
q_4 = \left\lfloor \frac{r_2}{r_3} \right\rfloor & r_2 = q_4\, r_3 + r_4 & r_4 = r_2 - q_4\, r_3 \\
q_n = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor & r_{n-2} = q_n\, r_{n-1} + r_n & r_n = r_{n-2} \\
 & & \quad - q_n\, r_{n-1} \\
q_{n+1} = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor & r_{n-1} = q_{n+1}\, r_n + 0 & r_n = r_{n-1} / q_{n+1}
\end{array}$$

Figure 3. Extended Euclidean Algorithm.
(https://mathworld.wolfram.com/EuclideanAlgorithm.html)

The left side of the figure represents the Euclidean Algorithm, which is used to find the **greatest common divisor (gcd)** of two integers.[3] This is represented in the form (a, b). The right side of the figure shows the extension of the algorithm, which uses backsolving to figure out the multiplicative inverse. We can apply this to a difficult congruence problem in order to solve it.

$$39x \equiv 534 \pmod{49}$$

Our initial observation is that the gcd of 39 and 49 must be 1. We can confirm this using the Euclidean Algorithm. We start by writing the division algorithm for the two numbers.

$$49 = 39 \cdot 1 + 10$$

Then we follow the algorithm to get the gcd.

$$\begin{aligned}
39 &= 10 \cdot 3 + 9 \\
10 &= 9 \cdot 1 + 1 \\
9 &= 1 \cdot 9 + 0 \\
\text{gcd} &= 1
\end{aligned}$$

Next, we work backwards in order to find the multiplicative inverse.

$$10 = 49 - 39 = b - a$$

We can substitute in (b - a) for -39 in the next step.

$$\begin{aligned} 9 &= a - 3(b - a) \\ 9 &= 4a - 3b \end{aligned}$$

We substitute in (b-a) for -39 and (4a-3b) for 9.

$$\begin{aligned} 1 &= (b - a) - (4a - 3b) \\ 1 &= 4b - 5a \end{aligned}$$

Substitute 49 back in for b and 39 back in for a.

$$1 = 4 \cdot 49 + \ -5 \cdot 39$$

This means that

$$39(-5) \ \equiv 1 \pmod{49}$$

-5 (mod 49) is congruent to 44 (mod 49), which is easier to work with.

$$39(44) \ \equiv \ 1 \pmod{49}$$

Remember from the beginning of the problem that we are working with 534 (mod 49).

$$534 \ \equiv \ 44 \pmod{49}$$

Now that we have rewritten this as simply as possible, we use the multiplication property for linear congruences to solve for x.

$$\begin{aligned} &(39)(44)(44) \equiv 44 \pmod{49} \\ &x = 44 \cdot 44 \\ &x = 7504 \end{aligned}$$

Modular arithmetic is not always limited to 1 congruence equation or parameter. It also includes **systems of congruences**, written as

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Figure 4. System of Congruence.

Sometimes these can be solved intuitively, but with larger numbers and more parameters, a systematic algorithm is required. For this, we turn to an ancient Chinese theorem that was used to calculate the calendar and find the number of soldiers when marching in lines.[4] Nowadays, we have found more uses for this theorem, especially in cryptography and cybersecurity schema.

b. The Chinese Remainder Theorem

The theorem being described is the **Chinese Remainder Theorem**. Sometimes it is called the Sun Zhu Theorem after the Chinese mathematician who invented it. It tells us that there is always a unique solution for systems of congruences up to a certain modulus, and can be used to find said solution.[5]

The Chinese Remainder Theorem uses pairwise relatively prime positive integers as the modulus values n_1, n_2,..., n_k. **Relatively prime** (coprime) implies that two integers do not share any common factors other than 1, or (a, b) = 1. Pairwise relatively prime implies that every pair of integers a and b from the set of modulus values are coprime.

The system of congruences has a unique solution modulo $P = n_1 n_2 ... n_k$. For each congruence equation, the number is congruent to P divided by the original congruence modulo[6]. We obtain P_1, p_2,..., P_k which will be used to find Q_1, Q_2,..., Q_k. Then every modulo expression will be rewritten as

$$\begin{aligned} P_1Q_1 &\equiv 1 \pmod{n_1} \\ P_2Q_2 &\equiv 1 \pmod{n_2} \\ &\vdots \\ P_kQ_k &\equiv 1 \pmod{n_k} \end{aligned}$$

Figure 5. Pairwise notation.

Our final expression congruent modulo N will be equal to

$$x \equiv a_1P_1Q_1 + a_2P_2Q_2 + a_3P_3Q_3 \pmod{N}$$

Figure 6. Solution to Chinese Remainder Theorem.

We involve our a_1, a_2,..., a_k in the final expression. The roundabout method gives us our solution (which can be represented as an equivalence class) of our system of congruences. Sometimes, the Extended Euclidean Algorithm will be used for intermediate steps while finding the multiplicative inverses of the numbers modulo n_1, n_2,..., or n_k.

Let us explore this method by solving the system of congruences portrayed below:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{7} \end{aligned}$$

Our P is equal to 105, which is the product of the n_1, n_2, and n_3 values. Dividing by the original congruence modulos we obtain

$$P_1 \equiv 35,\ P_2 \equiv 21,\ P_3 \equiv 15$$

Then we rewrite this as

$$\begin{aligned} 35Q_1 &\equiv 1 \pmod{3} \\ 21Q_2 &\equiv 1 \pmod{5} \\ 15Q_3 &\equiv 1 \pmod{7} \end{aligned}$$

These are all fairly easy to solve, so we can avoid using the Extended Euclidean Algorithm.

$$\begin{aligned} &2Q_1 \equiv 1 \pmod{3} \rightarrow Q_1 \equiv 2 \pmod{3} \\ &Q_2 \equiv 1 \pmod{5} \\ &Q_3 \equiv 1 \pmod{7} \end{aligned}$$

Now we write our final expression congruent modulo N. We simplify the congruence equation to obtain our value for x.

$$\begin{aligned} x &\equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 4 \cdot 15 \cdot 1 \pmod{105} \\ x &\equiv 140 + 63 + 60 \pmod{105} \\ x &\equiv 263 \pmod{105} \\ x &\equiv 53 \pmod{105} \end{aligned}$$

So the equivalence class, or solution set, for x is $x = 53 + 105t$, where t belongs to the set of positive and negative integers. The residue is $x = 53$. Regardless of harder problems with larger numbers, different expressions, and more congruence equations (parameters), evidently the process is inherently basic. The proof of the Chinese Remainder Theorem is not as simple.

Although there are other methods for solving systems of congruences, the Chinese Remainder Theorem is the most systematic and always works. Other techniques may involve substitution or trial and error – methods that fall apart with increasing difficulty.

c. Application of the Chinese Remainder Theorem: Cryptography

The remainder of this paper will concentrate on the application of the Chinese Remainder Theorem to **cryptography**. Cryptography is the art and science of keeping information secure from unintended audiences by using **encryption**, or encoding it.[7] Ancient cryptography included the Caesar cipher, an attempt at encoding data by shifting every letter in the alphabet one to the right. It also included the polyalphabetic cipher, which shifted every letter according to a code word. This was more secure, although both parties had to know the code word in advance.

Modern cryptography is based in technology and cybersecurity. Security is no longer dependent on the secrecy of the encryption method or algorithm, but only on the secrecy of **keys**. The new **ciphers** (encryption algorithms) are rooted in complex number theory, specifically modular arithmetic and application of prime numbers. We are going to focus on **RSA encryption**, a certain type of cipher, and applying the Chinese Remainder Theorem to RSA structures.

APPLICATION TO CRYPTOGRAPHY

a. RSA Encryption

Encryption uses a specific key to map a message to a ciphertext message. **Decryption** is the process of decoding a message, and relies on applying either the same key or a different key.[8] In RSA encryption, the keys used for encryption and decryption are related. Ronald L. Rivest, Adi Shamir, and Len Adleman were the first cryptographers to connect information security to modular exponentiation in 1977. This was a novel concept as the process of raising a number to an exponent, dividing by the modulus, and outputting the remainder yields an irreversible outcome. Given the exponent, modulus, and new value that is obtained, the original number cannot be derived.

$$A^{e} \pmod{N} \equiv c$$

In other words, c, in the congruence equation above, cannot be easily decrypted without knowing the original number A.

However, a person who has access to the original number could easily work backwards to obtain it again. Letting d equal to an integer such that

$$c^{d} \pmod{N} \equiv A$$

then applying a new function

$$A^{ed} \pmod{N} \equiv A$$

is a surefire way to reverse the exponentiation. So the last puzzle piece to RSA encryption involves a reliable (replicable, accurate) algorithm to generate a number d.

The optimal way to do this involves **Euler's totient function**, φ (pronounced phi). This is a high order **arithmetic function** that is prevalent in number theory. The totient function denotes the number of positive integers that are relatively prime to a number N.[9] It relies on knowing the prime factorization, which will always involve 2 prime factors.[9] When N is equal to p times q, φ(pq) equals (p-1) times (q-1) under all circumstances where p and q are prime. As finding a number's prime factorization is a **fundamentally hard problem**, but multiplying p times q together is simple to do even for very large inputs, this is the key to RSA Encryption.

We start with Euler's Theorem:[10]

$$\mathtt{A}^{\phi(\mathtt{N})} \equiv 1 \pmod{\mathtt{N}}$$

Then we manipulate as follows.

$$\mathtt{A}^{\mathrm{k}\phi(\mathtt{N})} \equiv 1 \pmod{\mathtt{N}} \rightarrow \mathtt{A} \cdot \mathtt{A}^{\mathrm{k}\phi(\mathtt{N})} \equiv \mathtt{A} \pmod{\mathtt{N}} \rightarrow \mathtt{A}^{\mathrm{k}\phi(\mathtt{N})+1} \equiv \mathtt{A} \pmod{\mathtt{N}}$$

This process yields an equation for finding e. Remember our original equation:

$$\mathtt{A}^{\mathrm{ed}} \pmod{\mathtt{N}} \equiv \mathtt{A}$$

Now we set the exponent portion of the congruences equal to each other.

$$\mathrm{ed} = \mathrm{k}\phi(\mathtt{N}) + 1$$

Divide by e on both sides. Our equation for d is as follows:

$$\mathrm{d} = \frac{\mathrm{k}\phi(\mathtt{N}) + 1}{\mathrm{e}}$$

Without knowing the original numbers multiplied together, p and q, an infiltrator to the system will not be able to compute the totient function. Going the other way (from the receiving party to the encryptor) relies on the power of the congruence equation. Both have a stunning irreversibility that makes this system so secure.

In order to make sense of the plethora of information above, we can dive into an example that shows RSA in action. Imagine a banker, John, that is interested in communicating with a client, Helen. John generates 2 random prime numbers: p = 59 and q = 71. Next he multiplies them together to get N = 4189. This operation is easy to do, but challenging to reverse. φ(4189) is comparable to doing φ(59) times φ(71), resulting in a number (59 - 1)(71 - 1) = 4060. John picks an exponent e = 9 to operate with. He computes d by plugging into the formula from earlier:

$$d = \frac{8 \cdot \phi(4189) + 1}{9}$$

In this case, k = 8 – this is the value that makes d a whole number. The arithmetic above comes out to d = 3609. After doing these steps, he is ready to send information over to Helen.

John has to send Helen the values for N and e, and omit the rest of the values for p, q, k, and d. Helen wants to send John a secret message A. This may be a string of characters that has been converted to a number. Let us say A = 73. She does this by computing according to the following relationship:

$$A^e \pmod{N} \equiv c$$

She gets 3636 for her encryption c, which she sends back to John. Now figuring out the message is easy for John. He applies the formula:

$$c^d \pmod{N} \equiv A$$

Surely enough, A is 73 which is what Helen sent him. After all the mathematical manipulation, the end result is still the same. Nowhere during John and Helen's communication could the message be interpreted because John held the key pertaining to retrieving it.

RSA encryption is not perfect. It is limited by complexity of the key creation, since it is hard to generate large primes efficiently.[11] Another issue other than the processing power is the slowness of speed, which can be attributed to the sheer amount of calculation and series of steps. Keeping that in mind, the RSA cryptosystem is still one of the best implemented security frameworks. Now we are going to introduce an application of the Chinese Remainder Theorem to connect cryptosystems resulting in a possibility for **RSA networks.**

b. Connecting Cryptosystems

With the model perpetuated above, only one person holds access to the key. That one person can receive information from many sources. Perhaps there is a different situation, where there are two keyholders from different cryptosystems. They may each define their own keys according to specific modulo N_1 and N_2. What if they wanted to share sources, or data according to different congruence structures?

The Chinese Remainder Theorem can come into play when building these connections. Expanding on the example from above, now suppose a banker John has a client Helen, and another banker Rob has a client Rose. They may each define their own RSA situations using random number generators for inputs p_1 and q_1, and p_2 and q_2 respectively. Keeping the data the same for John and Helen's communication, now we can add data for Rob and Rose's communication.

Exchange between John and Helen	Exchange between Rob and Rose
$p_1 = 59$	$p_2 = 103$
$q_1 = 71$	$q_2 = 113$
$e_1 = 9$	$e_2 = 5$
$N_1 = 4189$	$N_2 = 103 \cdot 113$ $N_2 = 11639$
$d_1 = 3609$	$\phi(11639) = 11424$ $d_2 = \frac{11424 + 1}{5}$ $d_2 = 2285$
$A_1 = 73$	$A_2 = 119$

$c_1 = 3636$	$119^5 \pmod{11639} \equiv c_2$ $c_2 = 1787$ $1787^{2285} \pmod{11639} \equiv 119$

Figure 7. Exchanges in Unique RSA Cryptosystems.

As we can see from the chart, Rob and Rose's communication was successful because Rob could use the key to figure out Rose's message. This results in the same number that she sent him at the end of the exchange.

Evidently 2 cryptosystems have been developed, each with their own data.

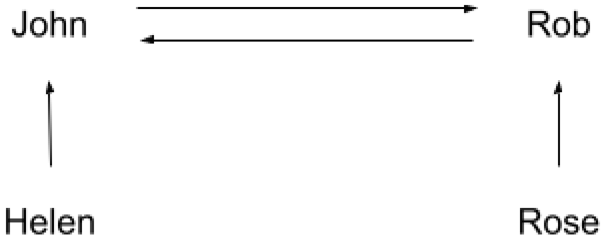


Figure 8. Simple Network of RSA Cryptosystems

Now the Chinese Remainder Theorem can be used to combine that data into one major cryptosystem. The system of congruence equations will be the following:

$$x \equiv 119 \pmod{11639}$$
$$x \equiv 73 \pmod{4189}$$

We have done the mathematics to solve this complex problem portrayed below. All of the techniques that are used have been discussed throughout the paper.

$$P_1 = 4189,\ P_2 = 11639$$

$$4189Q_1 \equiv 1 \pmod{11639}$$
$$11639Q_2 \equiv 1 \pmod{4189}$$

$11639 = 4189 \cdot 2 + 3261$
$4189 = 3261 \cdot 1 + 928$
$3261 = 928 \cdot 3 + 477$
$928 = 477 \cdot 1 + 451$
$477 = 451 \cdot 1 + 26$
$451 = 26 \cdot 17 + 9$
$26 = 9 \cdot 2 + 8$
$9 = 8 \cdot 1 + 1$
$8 = 1 \cdot 8 + 0$

$3261 = 11639 - 4189 \cdot 2 = b - 2a$
$928 = a - (b - 2a) = 3a - b$
$477 = (b - 2a) - 3(3a - b) = 4b - 11a$
$451 = (3a - b) - (4b - 11a) = 14a - 5b$
$26 = (4b - 11a) - (14a - 5b) = 9b - 25a$
$9 = (14a - 5b) - 17(9b - 25a) = 439a - 158b$
$8 = (9b - 25a) - 2(439a - 158b) = 325b - 903a$
$1 = (439a - 158b) - (325b - 903a) = 1342a - 483b$
$1 = 1342 \cdot 4189 - 483 \cdot 11639$

$(1342)(4189) \equiv 1 \pmod{11639}$
$Q_1 \equiv 1342 \pmod{11639}$

$11639Q_2 \equiv 1 \pmod{4189}$
$3261Q_2 \equiv 1 \pmod{4189}$

$4189 = 3261 \cdot 1 + 928$
$3261 = 928 \cdot 3 + 477$
$928 = 477 \cdot 1 + 451$
$477 = 451 \cdot 1 + 26$
$451 = 26 \cdot 17 + 9$
$26 = 9 \cdot 2 + 8$
$9 = 8 \cdot 1 + 1$
$8 = 1 \cdot 8 + 0$

$928 = 4189 - 3261 = b - a$
$477 = a - 3(b - a) = 4a - 3b$
$451 = (b - a) - (4a - 3b) = 4b - 5a$
$26 = (4a - 3b) - (4b - 5a) = 9a - 7b$
$9 = (4b - 5a) - 17(9a - 7b) = 123b - 158a$
$8 = (9a - 7b) - 2(123b - 158a) = 325a - 253b$
$1 = (123b - 158a) - (325a - 253b) = 376b - 483a$
$1 = 376 \cdot 4189 - 483 \cdot 3261$

$(-483)(3261) \equiv 1 \pmod{4189}$
$(3706)(3261) \equiv 1 \pmod{4189}$
$Q_2 \equiv 3706 \pmod{4189}$

$x \equiv 119 \cdot 4189 \cdot 1342 + 73 \cdot 11639 \cdot 3706 \pmod{48755771}$
$x \equiv 14816566 \pmod{48755771}$

Reversing the Chinese Remainder Theorem is easy. Finding the residue modulo N_1 and N_2 will result in the original secrets A_1 and A_2 which stand for the messages. Moreover, cryptographic schema such as this one do not have to be limited to 2 parties or 2 data values. But they should make sure to keep a thread of reversibility going so that the effects of merging systems can be undone to reveal the original messages. Here is another example of a more intricate network:

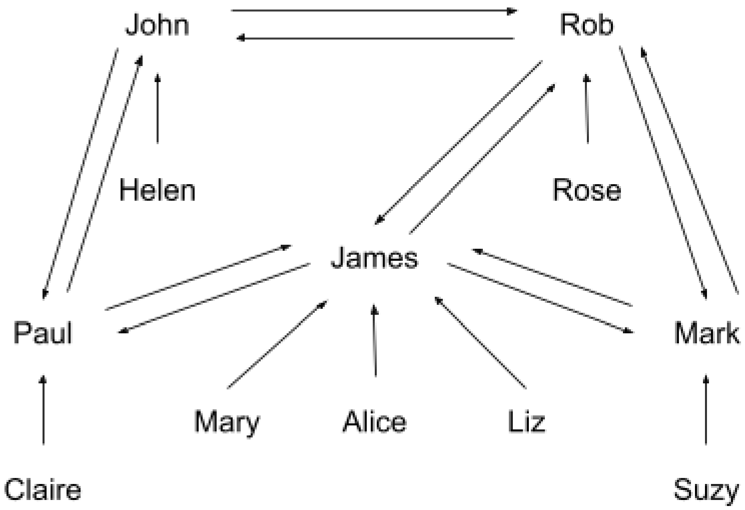


Figure 9. Elaborate Network of RSA Cryptosystems

In Figure 9, John, Rob, Mark, Paul, and James are bankers. Helen, Claire, Rose, Suzy, Mary, Alice, and Liz are all clients. Evidently, James has more business than the other bankers, but focuses on maintaining mutually beneficial relationships with the other financiers. They share data in multiple ways, which creates this web of communications or connections.

The most resourceful use of these resulting cryptographic systems would be for secret sharing among different entities. Other potential uses would be to improve storage and better organize information. In this way, using the Chinese Remainder Theorem in conjunction with RSA functionality is a highly potent solution to amalgamation of companies and their networks (not just limited to bankers). It is also a vigorous solution for government military branches working together in times of war crises.

CONCLUSION

Application of the Chinese Remainder Theorem as seen above should be further explored as it relates to secret sharing. Simulation techniques can be developed using a coding language such as Python with built in random number generators. These simulations would encapsulate a reasonable number of cryptosystems – perhaps 4, 5, or 6 of them – each with their own data (ranging from 15 to 30 successful communications).

Besides the direct benefit of exploring cryptographic networks introduced in this paper, simulating data en masse can lead to new discoveries in prime number theory. Mathematicians are still searching for a proof of the Riemann Hypothesis, which asserts that "non-obvious" zeroes of the zeta function are complex numbers with a real part ½. This is one of the Millennium Problems, which have $1 million prizes attached to them. Additionally, there is an ongoing search for a formula to model the exact prime number distribution (currently a formula only exists for the average distribution, called the prime number theorem). As cultivating a list of primes has generated little success, analyzing unconventional data in a modulus setting is a good area of research for the future.

Overall, there are tremendous implications of this new concept involving the Chinese Remainder Theorem. Certainly, we can dive deeper and see if the ramifications can be even greater in the future.

Works Cited

1. *Modular Arithmetic.* Brilliant. Retrieved February 23, 2021, from https://brilliant.org/wiki/modular-arithmetic/
2. Shoup, V. (2008). A Computational Introduction to Number Theory and Algebra, Version 2. Retrieved February 23, 2021, from https://shoup.net/ntb/ntb-v2.pdf
3. The Euclidean Algorithm and Multiplicative Inverses. *University of Utah*. Retrieved February 23, 2021, from https://www.math.utah.edu/~fguevara/ACCESS2013/Euclid.pdf
4. Lac, Ja. (2008). Chinese remainder theorem and its applications. *CSUSB Scholar Works*. Retrieved February 23, 2021, from https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=4457&context=etd-project
5. Lynn, B. The Chinese Remainder Theorem. *Stanford University*. Retrieved February 23, 2021, from https://crypto.stanford.edu/pbc/notes/numbertheory/crt.html
6. The Chinese Remainder Theorem. *Loyola University in Chicago.* Retrieved February 23, 2021 from http://gauss.math.luc.edu/greicius/Math201/Fall2012/Lectures/ChineseRemainderThm.article.pdf
7. Simpson, S. (1997) Encryption. *The University of Texas at Austin.* Retrieved February 23, 2021 from https://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/history.html
8. Preetha, M & Nithya, M. (2013) A Study and Performance Analysis of RSA Algorithm. *International Journal of Computer Science and Mobile Computing*, 2(6), 126-139. Retrieved February 23, 2021 from https://www.ijcsmc.com/docs/papers/June2013/V2I6201330.pdf
9. Weisstein, E. Totient Function. *Wolfram MathWorld*. Retrieved February 23, 2021 from https://mathworld.wolfram.com/TotientFunction.html
10. *Euler's Theorem.* Brilliant. Retrieved February 23, 2021 from https://brilliant.org/wiki/eulers-theorem/
11. NaQi, Wei, W., Zhang, J., Wang, W., Zhao, J., Li, J., Shen, P., Yin, X., Xiao, X., Hu, J. (2013) Analysis and Research of the RSA Algorithm. *Information Technology Journal*, 12, 1818-1824. https://doi.org/10.3923/itj.2013.1818.1824

GLOSSARY

Modular arithmetic - A system of arithmetic for integers where numbers “wrap around” a certain modulus. The primary focus is on working with remainders. This is a subcategory under the broader field of number theory, but has a variety of applications, which include modern-day cryptography, computer science programs, checking serial number identifiers, and analyzing repeating phenomena in nature (biology, chemistry, and physics).

Linear congruence - One of the basic structures of modular arithmetic. We say a is “equivalent” to b modulo n if both integers have the same remainder after division by n. Another way of understanding this is that subtracting a from b should always result in an integer that is perfectly divisible by n. Linear congruences have an abundance of properties associated with them.

Equivalence relation - Are binary, and have properties of reflexivity, symmetry, and transitivity. Binary implies that they involve interaction from 2 sets. Linear congruences can be viewed as equivalence relations because each number is being operated on by a modulo, which partitions the integer realm into a remainder set and an ordinary set. All numbers that give the same remainder form what is known as an equivalence class.

Extended Euclidean Algorithm - The Euclidean Algorithm repeatedly applies the division algorithm, but shifts the inputs to the left every time. This results in finding the gcd of 2 numbers once the remainder has been eliminated. The Extended Euclidean Algorithm uses the process from the Euclidean Algorithm to backtrack. The end result is the form ax + by = gcd(a, b), which reveals the multiplicative inverse for a number modulo n.

Multiplicative inverse - The multiplicative inverse of a real number x is a number that results in 1 when multiplied together with x. In traditional arithmetic, this involves taking the reciprocal of the number x. In modular arithmetic, the multiplicative inverse is actually another integer and varies depending on prime number theory.

Greatest Common Divisor (gcd) - Represented in the form gcd(a, b). The gcd is the largest positive integer that divides both integers. It is also called the greatest common factor (gcf) and the greatest common measure. The gcd is one of the most important units of number theory, although it is also taught at an elementary school level.

System of congruences - When there are multiple congruence equations (parameters), and they all have to hold true for a number x. There are multiple solutions for these types of equations, involving intuition, substitution, and the Chinese Remainder Theorem.

Chinese Remainder Theorem - An ancient Chinese theorem that was used to calculate the calendar and find the number of soldiers when marching in lines. It has also been called the Sun Zhu Theorem after the Chinese mathematician that invented it. Interestingly enough, there was a variant of the theorem in ancient Egypt. The Chinese Remainder Theorem states assert that for pairwise coprime integers in modular congruences, there is one number x which is a solution. It also explores how to find that number x.

Relatively prime - A synonym for the word coprime. Relatively prime integers do not share any factors in common other than 1. The gcd(a, b) if a and b are coprime is 1.

Cryptography - The art and science of keeping information secure from unintended audiences. It is the practice of constructing and analyzing secrecy protocols to keep other parties, also known as adversaries, from seizing private messages. Ancient cryptography involved sending letters or numbers across distances, whereas modern cryptography is computerized and primarily concerned with online cryptosystems.

Encryption - Encoding information in order to hide it from other parties. Encryption utilizes a variety of algorithms to change the original message, known as plaintext, to ciphertext which is its disguised state.

Key - A value or parameter that specifies the transformation of plaintext and ciphertext (encryption), and ciphertext into plaintext (decryption). The key is only known to the authorized party or parties.

Cipher - The name given to encryption algorithms. Ancient cryptographic ciphers included the Caesar cipher and polyalphabetic cipher, among others. These methods relied on transformations to the original text such as letter shifts, number to letter encoding, and mathematical operations on numbers. The new ciphers involve complex number theory. Many of them involve modular arithmetic like the RSA encryption system.

Decryption - The process of decoding a message. Decryption uses algorithms to change the encrypted ciphertext back into plaintext. It may involve the same key, a related key, or an entirely different key to perform this transformation.

RSA encryption - A commonly used cryptosystem since its creation by Ronald L. Rivest, Adi Shamir, and Len Adleman in 1977 (hence its name which stands for Rivest–Shamir–Adleman). RSA encryption relies on modular exponentiation to generate ciphertexts that are irreversible without the original key. It is known as a public-key cryptosystem because the encryption key is public, whereas the decryption key is hidden from everyone except the original cryptographer. It uses a modified version of Euler's Theorem, which in itself is a play on Fermat's Little Theorem.

Euler's totient function - Counts the positive integers up to a given integer N that are relatively prime to N. Solving this problem is hard for all numbers unless their prime factorization is known. Then φ (pronounced phi) is equal to the product of each of the prime factors minus 1. Euler's totient function is part of prime number theory, and is a type of arithmetic function.

Arithmetic function - May also be known as a number-theoretic function. It is any function whose domain is the positive integers and whose range is over the set of complex numbers. Some of the most prominents examples in number theory include Euler's totient function, tau and sigma functions, and the Mobius function.

Fundamentally hard problem - Any problem that is hard to solve within a reasonable timespan. A lot of cryptographic reasoning and development of algorithms depends on creating fundamentally hard problems. Although they can be figured out within a period such as 100 years, by this time information can be moved to other cryptosystems or is no longer relevant.

RSA networks - An extension of the Chinese Remainder Theorem to link RSA cryptosystems. Can be used for secret sharing among multiple entities, eliminating the issue of one person having access to data within his/her security framework. This is a novel concept which the paper leads up to. It can potentially be used to collect data for induction, leading to advancements in prime number theory, not to mention greater security, optimization of storage, and cultivating government and business relationships.