Lagrange's Theorem and The RSA Encryption Algorithm A Final Course Output in ABSTAL1

John Paul Guzman
De La Salle University
2401 Taft Avenue, Manila

1 Introduction

The RSA encryption algorithm is one of the most commonly used encryption algorithms that we use in our day to day lives. It enables people to transfer sensitive data (passwords, credit card information, home addresses, etc.) over the wire in such a way that these data can be read only by its intended recipient. It secures sensitive data from so-called "man-in-the-middle" attacks wherein malicious third-party eavesdrops on the communication between two parties with the intent of stealing sensitive information [1].

2 Preliminary Concepts

Definition 2.1: Partition - The partition P of the set S is a set of subsets P_i of S such that the union of all P_i's equals S, and for any $i \neq j$, Pi and Pj are disjoint.

Example 2.2: The set of natural numbers is partitioned by the set of odd numbers and the set of even numbers.

Definition 2.3: Group - The tuple $(G, \circledast)$ is a group if it satisfies the four properties:

1. Closure - For any a, b in G, $a \circledast b$ in G.
2. Associativity - For any a, b, c in G, $(a \circledast b) \circledast c = a \circledast (b \circledast c)$.
3. Identity - There exists e in G such that for any a in G, $a \circledast e = a = e \circledast a$.
4. Inverse - For any a in G, there exists a^{-1} in G such that $a \circledast a^{-1} = e = a^{-1} \circledast a$.

Example 2.4: The set of integers under addition forms the group called $(\mathbf{Z}, +)$.

Example 2.5: The set of integers under addition modulo n forms the group called $(\mathbf{Z}_n, +)$.

Definition 2.6: Order of a group - The order of the group $(G, \ast)$ is $|G|$.

Example 2.7: The order of the group $(\mathbf{Z}_n, +)$ is n.

Definition 2.8: Subgroup - H is a subgroup of the group $(G, \ast)$ if H is a subset of G and $(H, \ast)$ forms a group.

Example 2.9: The set of even integers, $\{2k \mid k \in \mathbf{Z}\}$, forms a subgroup of $(\mathbf{Z}, +)$.

Definition 2.10: (Left) Coset - $g\,H$ is a left coset of the subgroup $(H, \ast)$ if $g \in G$ and $g\,H = \{g \ast h \mid h \text{ in } H\}$.

Example 2.11: $\{3 + 2k \mid k \in \mathbf{Z}\}$ is the left coset of $g = 3$ and the subgroup in Example 2.9.

Theorem 2.12: Lagrange's Theorem - If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

> Proof: Suppose H is a subgroup of a finite group G. G can be partitioned into a set of k left cosets of H, and each coset has the same cardinality, and thus $|G| = k\,|H|$ or $|H|$ *divides* $|G|$.

Definition 2.13: Multiplicative group of integers modulo n ($\mathbf{Z}_n^*$) - $\mathbf{Z}_n^*$ is the group formed from the set of integers that are relatively prime to n with multiplication modulo n.

Definition 2.14: Euler's φ-function - φ is the function defined as $\varphi(n) = |\mathbf{Z}_n^*|$.

Theorem 2.15: Euler's Theorem - If a and n are relatively prime, then $a^{\varphi(n)} \equiv 1 \bmod n$.

> Proof: Suppose a and n are relatively prime. Then, a is an element of $\mathbf{Z}_n^*$. Thus, a generates a cyclic subgroup $\langle a \rangle$ with some order m. *Moreover,* $a^m = e$. By Lagrange's Theorem, $|\langle a \rangle|$ divides $|\mathbf{Z}_n^*|$ or m divides $\varphi(n)$. Thus for some integer k, $\varphi(n) = k\,m$. Therefore $a^{\varphi(n)} = a^{k\,m} = a^{m\,k} = e^k = 1^k = 1$.

Illustration 2.16: Let $a = 13$, $n = 17$. Since 17 is a prime number, $\varphi(17) = 16$. It is easy to verify that the congruence $13^{16} \equiv 1 \bmod 17$ holds.

3 Application of Concepts Learned

The RSA encryption algorithm works as follows [2]:

1. The receiver picks two large prime numbers (p and q) and two integers (e and d) that satisfy the relation $e*d \equiv 1 \bmod \varphi(p*q)$. e is called the public key, while d is called the private key.
    a. Note that the values for d and $\varphi(p*q)$ could be easily computed by the receiver since he/she knows the prime factorization of p*q and φ has a property that states $\varphi(p*q) = \varphi(p)*\varphi(q) = (p-1)*(q-1)$ [3].
2. The receiver publicly announces two pieces of information: the product $p*q$, and the public key e.
3. The sender uses these two pieces of information to encrypt the message M (a string coded as an

integer) into the ciphertext C that satisfies $C \equiv M^e \bmod (p*q)$ and sends C to the receiver.

   a. Note that we assume the size of M must be less than $p*q$. If it's not, then the sender can split M into multiple chunks where the size of each chunk is less than $p*q$.

4. Finally, the receiver will then take C and reconstruct M using the following claim: $M \equiv C^d \bmod (p*q)$.

   Proof: In practice, It is safe to assume that M is relatively prime to $p*q$ since it is unlikely that M is a factor of p or q. Thus, we can use Euler's theorem in the following way: $M^{\varphi(p*q)} \equiv 1 \bmod (p*q)$. The claim follows from this and the definitions of p, q, e, d, M, C.

$$(C^d \equiv (M^e)^d \equiv M^{e*d} \equiv M^{1+k(\varphi(p*q))} \equiv M \times M^{\varphi(p*q)*k} \equiv M \times 1^k \equiv M) \bmod (p*q)$$

Now suppose that there were unwanted eavesdroppers that recorded the exchange. They would know the values for $p*q$, e, and C. However, they would be unable to reconstruct M since they do not have the value for the private key d. Furthermore, finding a value for d, without knowledge of the prime factors p and q, is computationally expensive since determining the value of $\varphi(p*q)$ requires some form of exhaustive search. Therefore it is computationally infeasible for large enough values of p and q [4]. Computing for the value of $\varphi(p*q)$ generally hard, but it can become trivial if one knows the prime factors p and q. This is why φ is called as a trapdoor function where p and q are its trapdoors [1].

4 Conclusion

Man-in-the-middle attacks are one of the biggest vulnerabilities of symmetric (shared key) encryption systems since those require the sender and receiver to agree on the shared key that will be used for both encrypting and decrypting messages. Unfortunately, they would need to communicate the shared key over the wire to establish an agreement. Thus, the third-party could simply keep a copy of the shared key, and then he/she will be able to decrypt further communication [1]. RSA is an asymmetric encryption algorithm which uses separate keys for encrypting and decrypting messages. It allows one to communicate encryption keys over the wire while being safe from man-in-the-middle attacks [5].

References

[1] Stallings, W. (1999). *Cryptography and network security: principles and practice*. Upper Saddler River, New Jersey: Prentice Hall.

[2] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126. doi: 10.1145/359340.359342

[3] Long, C. T. (1995). *Elementary introduction to number theory* (2nd ed.). Prospect Heights, Illinois: Waveland Press.

[4] Arora, S., & Barak, B. (2009). *Computational complexity A Modern Approach*. New York: Cambridge University Press. doi: 10.1017/CBO9780511804090

[5] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654. doi: 10.1109/tit.1976.1055638