INL/EXP-22-68303-Revision-0

Exploring Applied Cryptosystems to Formally Verify Security in Cyber-Physical Systems

August 2022

Sara Rose Logsdon

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/EXP-22-68303-Revision-0

Exploring Applied Cryptosystems to Formally Verify Security in Cyber-Physical Systems

Sara Rose Logsdon

August 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Final Edge of Poster

Exploring Applied Cryptosystems to Formally Verify Security in Cyber-Physical Systems

Sara Logsdon
University of Georgia

Mentor: Dr. Gregory Shannon
Idaho National Laboratory

National & Homeland Security

1. Abstract

This project aims to evaluate RSA as a method for public-key encryption for cyber-physical systems (CPS). As technology advances, cyber attacks are increasing, and with them, the need for cybersecurity advances;[1] the average cost for cybercrime in the world was estimated at $6 trillion in 2021.[2] A public-key cryptosystem that has been around since 1977, RSA has recently garnered some critiques for its fragility, computational cost, and lazy implementation.[3] In this project I will review the mathematical derivation of RSA, analyze the practical implications of such mathematical framework for the security of RSA, and propose a formal methods based approach to verify encryption schemes for CPS.

2. Motivation

Recent technological advancements are providing a catalyst for the Fourth Industrial Revolution, Industry 4.0, by integrating the internet of things (IoT), artificial intelligence, and smart automation to physical systems.[4] It was estimated that there were 50 billion interconnected devices in 2020. This quantity is increasing exponentially, and with it, attack vectors of CPS increases as well. This has caused cybercrime to increase faster than ever. "Cybersecurity Ventures" estimates that in 2021, businesses will fall prey to cyber attacks every 11 seconds, up from every 40 seconds in 2016.[5]

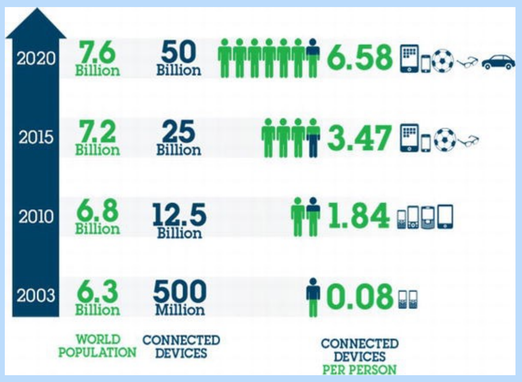


Fig 1. The overall world population and connected devices by 2020

3. About Applied Cryptosystems– RSA Method

RSA is an **asymmetric** encryption algorithm. This means that it uses a publicly known key for encryption, but uses a different key, known only to the intended recipient, for decryption. In our case, the private key is p, q, and d, and the public key is n and e. For example, when Sara Logsdon is attempting to connect to her Idaho National Laboratory VPN from home, she uses the public key n and e of the server to authenticate herself, and the server uses the private key p, q, and d to decrypt the authentication message from Sara. In this way, Sara's data remains in the established encrypted tunnel for all communications between her and the server.

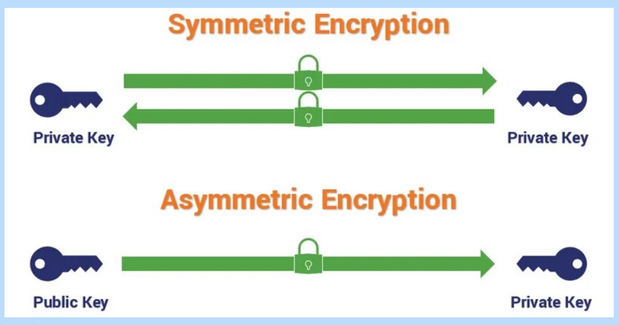
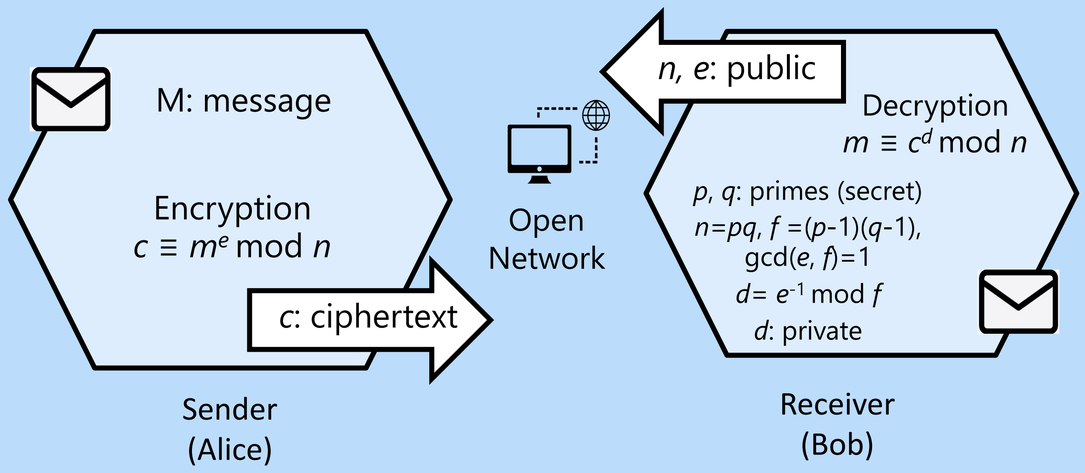


Fig 2. Symmetric versus asymmetric encryption

4. Methods & Mathematics[6]



Example: Bob chooses primes p=47 and q=67 and then computes n=(47)(67)=3149. He chooses e = 5. Compute f=(47-1)(67-1)= 3036.

We verify that gcd(5, 3036)=1 using the Euclidean Algorithm:
3036 = (607)5 + 1 → 5=(5)1+0, so indeed gcd(5,3036)=1.

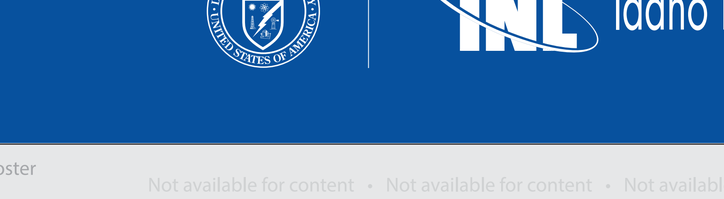
Bob must compute $d = 5^{-1} \pmod{3036}$ = multiplicative inverse of 5 modulo 3036 = an integer d s.t. $5d \equiv 1 \pmod{3036}$.
Working backwards through the Euclidean Algorithm we see that
3036 + (-607)5 = 1 →
0 + (-607)5 ≡ 1 (mod 3036)
→(2429)5 ≡ 1 (mod 3036)
(Here we added 3036 to -607 to get 2429)
Thus we have d=2429.

Bob now has p, q, n, e, and d. He keeps p, q, and d secret and makes n and e public so that Alice can send him an encrypted message.
If Alice wants to send "HI" to Bob, letting A→01, B→02, … "HI" gives m=0809=809.
Then Alice takes Bob's encryption key and computes
$c \equiv m^e \pmod{n} \equiv 809^5 \equiv 2522 \pmod{3149}$
For computing powers modulo n we use successive squaring.
$5 = 4+1 = 2^2+2^0 \rightarrow$
$809^5 \equiv 809^{4+1} \equiv (809^2)^2\,(809)^1 \equiv (654481)^2\,(809) \pmod{3149}$
We continually reduce modulo 3149 until we achieve
$(654481)^2\,(809) \equiv \ldots \equiv 2522 \pmod{3149} \equiv c$.
Alice chooses c= 2522 (0<2522<3149).

Alice sends her cipher text c to Bob. Bob can now decrypt Alice's message as $m \equiv c^d \pmod{n} \equiv 2522^{2429} \equiv 809 \pmod{3149}$
Bob identifies that m = 809 (0<809<3149). He recovers Alice's "HI."

5. Further Research: Formal Methods & CPS

Formal methods refers to constructing abstract representations of software and using advanced mathematical theorems to prove the software does what one wants it to. This type of formal verification enables programmers to **prove** their software does not contain errors. RSA encryption *has* been verified in the Isabelle/HOL theorem prover.



Scan for the Isabelle/HOL verification code![7]

RSA allows users to pick their own many parameters, possibly in an easily factorable way. Additionally, we observe that the larger our p and q, the more challenging the key is to crack. As cybercrime evolves, it demands longer, more computationally expensive keys. While RSA is secure (even verified in Isabelle), the computational cost exceeds the security. This opens the door for other encryption schemes for computationally limited systems, and begins the discussion of the role that formal methods may play in verifying such a scheme.

1. L.O. Mailloux and M. Gramaila, 2018
2. Sviatun, Olena and Goncharuk, 2021
3. Lila Kee, Forbes, 2021
4. Klaus Schwab, 2017
5. Hesham Alshaikh, 2020
6. Amy Kosek, 2015
7. Christina Lindenberg and Kai Wirt, 2021

Fig 1. Ismail, Yasser, 2019
Fig 2. Wagner, Lane 2020

www.inl.gov

Idaho National Laboratory

Final Edge of Poster