A discovery based approach for learning RSA

Tamara Veenstra

University of Redlands (Emerita) & IDA-CCR La Jolla

May 12, 2025, Crypto Educators Meeting

Motivation

- With the advent of post-quantum cryptography, we might well ask if we should still teach RSA.
- The history is fascinating! (How often do you get to talk about impossible and revolutionary things in math class?!?)
- The math is fascinating!
- Main goal is to demo some of the discovery based activities for RSA from my open textbook
- But first a little history...

The history is fascinating!

Classified work at Government Communications Headquarters (GCHQ), declassified in 1997.

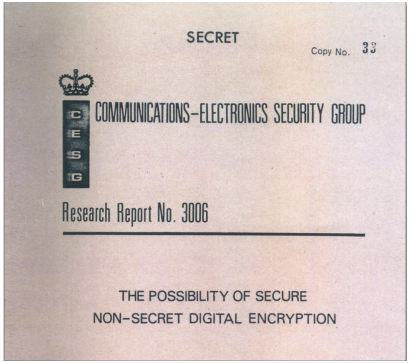
- James Ellis, 1970.
- Malcolm Williamson, 1973.
- Clifford Cocks, 1974.

Public History

- Whitfield Diffie, Martin Hellman, Ralph Merkle, 1976
- Ron Rivest, Adi Shamir and Leonard Adleman, 1978

James Ellis: 1970, declassified 1997

Ellis was inspired by an article about adding noise to an audio message to encrypt speech, to develop the **impossible** idea of public key cryptography.


SECRET

Copy No. 35

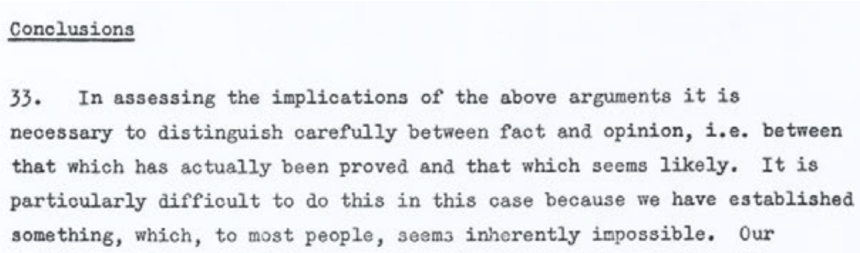
COMMUNICATIONS-ELECTRONICS SECURITY GROUP

Research Report No. 3006

THE POSSIBILITY OF SECURE
NON-SECRET DIGITAL ENCRYPTION

J.H. Ellis, Communications - Electronics Security Group, Government Communications Headquarters, Research Report No. 3006, The Possibility of Secure Non-Secret Digital Encryption, January 1970, declassified in 1997. link

Impossible!



Conclusions

33. In assessing the implications of the above arguments it is necessary to distinguish carefully between fact and opinion, i.e. between that which has actually been proved and that which seems likely. It is particularly difficult to do this in this case because we have established something, which, to most people, seems inherently impossible. Our

In 1987 GCHQ paper, Ellis writes about how impossible this idea seemed initially. (Later published externally, "The history of non-secret encryption", Ellis, J.H. *Cryptologia*; West Point Vol. 23, Iss. 3, (Jul 1999): 267.)

> *"It was obvious to everyone, including me, that no secure communication was possible without a secret key, ... Thus there was no incentive to look for something so clearly impossible."*

GCHQ Timeline

- 1970: James Ellis proposed the idea for public key cryptography.
- 1973: Clifford Cocks discovered ideas similar to the RSA algorithm.
- 1974: Malcolm Williamson developed ideas similar to the Diffie-Hellman key exchange.

In his 2021 induction into the Cryptologic Hall of Honor (with Ellis and Williamson) Clifford Cocks described how public key cryptography was

> *an idea that at the time seemed so outrageous there was even an effort to find a proof that it couldn't be done.*

link to video. (See times 2:25, 3:29)

Diffie-Hellman-Merkle: 1976

I. Introduction

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

- Whitfield Diffie, Martin Hellman, "New directions in Cryptography", IEEE Transactions on Information Theory, 22 (6): 644, 1976. link
- Photo taken from a talk by Martin Hellman, Stanford Seminar: The Evolution of Public Key Cryptography, video link.

New Directions in Cryptography: 1976

VII. Historical Perspective

While at first the public key systems and one-way authentication systems suggested in this paper appear to be unportended by past cryptographic developments, it is possible to view them as the natural outgrowth of trends in cryptography stretching back hundreds of years.

The last characteristic which we note in the history of cryptography is the division between amateur and professional cryptographers. Skill in production cryptanalysis has always been heavily on the side of the professionals, but innovation, particularly in the design of new types of cryptographic systems, has come primarily from the amateurs. Thomas Jefferson, a cryptographic amateur, invented a system which was still in use in World War II [2, pp. 192–195], while the most noted cryptographic system of the twentieth century, the rotor machine, was invented simultaneously by four separate people, all amateurs [2, pp. 415, 420, 422–424]. We hope this will inspire others to work in this fascinating area in which participation has been discouraged in the recent past by a nearly total government monopoly.

Martin Hellman: Revolutionary and Impossible!

Transcription of oral interview with Martin Hellman, conducted by Jeffrey Yost, November 2024. link

> *I start off by saying that public key cryptography is seen as revolutionary and of course it is a revolutionary concept.*
>
> ⋮
>
> *So, when I first described it to Feistel, in kind of a hurried way because he had a doctor's appointment, he said, 'You can't do that.'*

Similar comments from Martin Hellman in An Overview of Public Key Cryptography, IEEE Communications Society Magazine, 1978. link.

Rivest, Shamir, Adleman: 1978

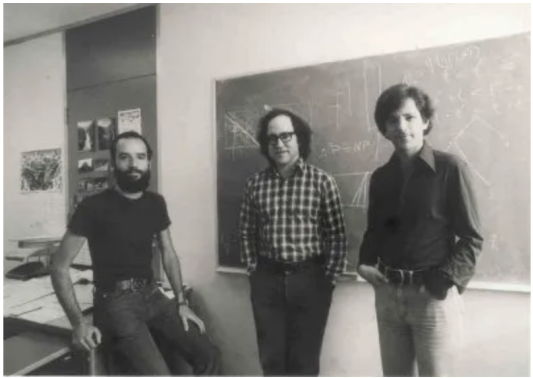


Photo accessed from National Cryptologic Foundation Website (website link) which states "Pictured in the photo - left to right: Adi Shamir, Ron Rivest, and Len Adleman. Photo courtesy of Dan Wright's RSA Algorithm course on imps.mcmaster.ca."

I. Introduction

The era of "electronic mail" [10] may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are *private*, and (b) messages can be *signed*. We demonstrate in this paper how to build these capabilities into an electronic mail system.

At the heart of our proposal is a new encryption method. This method provides an implementation of a "public-key cryptosystem", an elegant concept invented by Diffie and Hellman [1]. Their article motivated our research, since they presented the concept but not any practical implementation of such a system. Readers familiar with [1] may wish to skip directly to Section V for a description of our method.

R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Volume 21, Issue 2, pp120-126, 1978. (link)

History worth knowing!

So many things are possible just as long as you don't know they're impossible. *(Norton Juster, "The Phantom Tollbooth".)*

Public key cryptography is currently used so widely that it is important to remember how impossible and revolutionary it was at the beginning.

Guided Series of Activities for Exploring RSA

- Goal: Use the cryptography to motivate the math rather than as an application after the math.
- Guiding philosophy for my open textbook, Cryptology by Discovery, written for an intro crypto course, available on my website at link
- Most of the previous historical material and all activities that follow are from that textbook.
- Activities could be used in a wide range of classes (Cryptography, Number Theory, Abstract Algebra).

Demo from textbook (Backup screen shot)

5.4 A Number Trick

Let's start with another fun number game!

Exploration 5.4.1. Pick a secret x, then compute $y = x^5 \bmod 23$. Now take y and compute $z = y^9 \pmod{23}$. There is Sage code to help.

```
4   z=yy^9%23
5   pretty_print(html(r''' $y=%s^5 \equiv %s \pmod{23}$  '''% (xx,y
6   pretty_print(html(r''' $z=%s^{9} \equiv %s \pmod{23}$ '''% (yy,
7   #
8   #
9   #
10  #
11  #
12
```

Evaluate (Sage)

Enter x 6

$y = 6^5 \equiv 2 \pmod{23}$

$z = 2^9 \equiv 6 \pmod{23}$

Help | Powered by SageMath

What happened? Why?

▾ Hint

Examine $(x^5)^9 = x^{45} \pmod{23}$ for all x mod 23. What do you notice?

Definition 5.4.1. In general, we define a ***number trick*** to mean that we can find a d and e such that

$$(x^d)^e \equiv x \mod n$$

for all $x \bmod n$.

In order for such a d and e to exist we need to know if we can find an $a > 1$ such that $x^a \equiv x \pmod{n}$. In fact, we want to know all possible values of $a > 1$ that will work.

Investigation Time!

Time for you to explore this in Investigation: Power Patterns, Investigation: More Mod Patterns, and Investigation: Satisfying Two Mods.

Finding Patterns and Making Conjectures

Students use SageMath code (embedded in interactive cell in website, so no knowledge or access to SageMath is necessary) to make conjectures about when $x^a \equiv x \bmod n$ for all x. Activity from 5.11.2 Investigation: Power Patterns

5.11.2 Investigation: Power Patterns

1. Pick any number, x, between 2 and 17.

a. Compute $y = x^5 \pmod{19}$. Now compute $z = y^{11} \pmod{19}$. What's interesting about z? Why?

b. Compute $y = x^7 \pmod{19}$. Find a b such that $z = y^b \pmod{19}$ gives you the same interesting result as before for all x. That is, try all b in $1, 2, \cdots 19$ until you find one that works.

c. Compute $y = x^3 \pmod{19}$. Can you find a b such that $z = y^b \pmod{19}$ gives you the same interesting result as before? That is, try all b in $1, 2, \cdots 19$ until you find one that works.

2. Explain what the code below does. How does it relate to the earlier questions?

Sage Computation 5.11.2. Power Patterns.

```
n=19
pretty_print(html(r''' $x^a \equiv x \pmod{%s}$ if $a=$ '''% (n)))
for a in range(5*n):
    count=0
    for x in range(n):
        if x^a%n==x:
            count+=1
    if count==n:
        print("%s, " %a, end="")
```

Evaluate (Sage)

$x^a \equiv x \pmod{19}$ if $a =$
1, 19, 37, 55, 73, 91,

Help | Powered by SageMath

Prime Conjectures

- Students then explore these patterns for other prime numbers as an in-class activity. Students do quite well at making conjectures here!
- if p is a prime then $x^a \equiv x \bmod n$ for all x, if $a = 1 + (p-1)k$ for $k \in \mathbb{Z}$.
- Students can then explain why the previous number tricks worked! For example, $x^a \equiv x \pmod{19}$ if $a = 55$. So $(x^5)^{11} \equiv x \pmod{19}$ for all $x \bmod 19$.
- Then students are asked to make their own number tricks using these patterns! That is, find two different pairs of s and d such that $(x^s)^d \equiv x \pmod{19}$ for all $x \bmod 19$.

More Conjectures

So we ramp it up for homework! What about other n??

6. Use the Sage code in Sage Computation 5.11.2 to find all a such that

a. $x^a = x \pmod{55}$ for all x mod 55.

b. $x^a = x \pmod{77}$ for all x mod 77.

c. $x^a = x \pmod{143}$ for all x mod 143.

d. $x^a = x \pmod{221}$ for all x mod 221.

e. $x^a = x \pmod{323}$ for all x mod 323.

13. In the computational exercises, you explored many cases for when there are values for $a > 1$ such that $x^a = x \bmod n$ for all x mod n and what the pattern for those a values are when n is not prime. Write up the conjectures you have. Try to combine them into a single conjecture if possible!

14. Here's a new number trick algorithm. The encryption algorithm is $E(x) : y \equiv x^7 \bmod 55$. The decryption algorithm is $D(y) : x = y^{23} \bmod 55$. Explain why the number trick works. (Remember that you found all a such that $x^a \equiv x \bmod 55$ above.)

This is where it gets fun!

This really gets the students! Its substantially more interesting in the case $n = pq$. And maybe not what you're expecting.

$$x^a \equiv x \bmod n$$

where $a = 1 + mk$

n	p	q	m
22	2	11	10
26	2	13	12
33	3	11	10
39	3	13	12
55	5	11	20
65	5	13	12
187	17	11	80
221	17	13	48

This is where it gets fun!

This really gets the students! Its substantially more interesting in the case $n = pq$. And maybe not what you're expecting.

$$x^a \equiv x \bmod n$$

where $a = 1 + mk$

n	p	q	m	$\phi(n)$
22	2	11	10	10
26	2	13	12	12
33	3	11	10	20
39	3	13	12	24
55	5	11	20	40
65	5	13	12	48
187	17	11	80	160
221	17	13	48	192

More Conjectures

- We get to play with lots of experiments and conjectures here!
- if $n = pq$ is a prime then $x^a \equiv x \bmod n$ for all x, if $a = 1 + \text{lcm}(p-1, q-1)k$ for $k \in \mathbb{Z}$.
- Idea: $\mathbb{Z}/(pq)$ is not cyclic, so we need to know about the maximal order of elements not the order of the group.
- Quick Proof (if students have seen abstract algebra):

$$\mathbb{Z}/(pq) \cong \mathbb{Z}/(p) \times \mathbb{Z}/(q)$$

$$|ab| = \text{lcm}(|a|, |b|)$$

Theorem (Fermat's Little Theorem)

If p is a prime then $x^a \equiv x \bmod n$ for all x, if $a = 1 + (p-1)k$ for $k \in \mathbb{Z}$.

5.11.3 Investigation: More Mod Patterns [Activity to prove Fermat with binomial theorem mod p and induction]

Theorem (Not quite Euler's Theorem)

If $n = pq$ for distinct primes p,q then $x^a \equiv x \bmod n$ for all x, if $a = 1 + lcm(p-1, q-1)k$ for $k \in \mathbb{Z}$.

5.11.4 Investigation: Satisfying Two Mods [Activity for Chinese Remainder Theorem]

Thank you!

I'm happy to talk more about my textbook (and encourage anyone to use material from it!)

Questions?