Prime Polynomials

Daniel Klintworth

Prime Polynomials and RSA Encryption

Practical Applications in Encryption

A potential weakness in RSA

We Know...

Prime Numbers

2, 3, 5, 7, 11, 13, 17...

Polynomials

$a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n$

$x^2 + 2x + 5$

What even is a prime polynomial?

Factoring Polynomials

$x^2 + 5x + 6 = (x + 3) \cdot (x + 2)$

Factoring Polynomials

$x^2 + 5x + 6 = (x + 3) \cdot (x + 2)$

$x^3 + x^2 \qquad = x^2 \cdot (x + 1)$

Prime Polynomials

also: irreducible polynomials

$2x^5 + 30x^3 + 90$

$8x^7 + 7x^4 + 21x^2 - 15x + 22$

Caesar Cipher

Caesar Cipher

The textbook example for symmetric cryptography

Named after Gaius Julius Caesar

Caesar used it whenever he wrote something confidential

It was likely considered to be secure during its time

Caesar Cipher: Encryption

P	O	L	Y	N	O	M	I	A	L

Caesar Cipher: Encryption

P	O	L	Y	N	O	M	I	A	L
16	15	12	25	14	15	13	9	1	12

Caesar Cipher: Encryption

P	O	L	Y	N	O	M	I	A	L
16	15	12	25	14	15	13	9	1	12
19	18	15	2	17	18	16	12	4	15

Caesar Cipher: Encryption

P	O	L	Y	N	O	M	I	A	L
16	15	12	25	14	15	13	9	1	12
19	18	15	2	17	18	16	12	4	15
S	R	O	B	Q	R	P	L	D	O

Caesar Cipher: Decryption

S	R	O	B	Q	R	P	L	D	O

Caesar Cipher: Decryption

S	R	O	B	Q	R	P	L	D	O
19	18	15	2	17	18	16	12	4	15

Caesar Cipher: Decryption

S	R	O	B	Q	R	P	L	D	O
19	18	15	2	17	18	16	12	4	15
16	15	12	25	14	15	13	9	1	12

Caesar Cipher: Decryption

S	R	O	B	Q	R	P	L	D	O
19	18	15	2	17	18	16	12	4	15
16	15	12	25	14	15	13	9	1	12
P	O	L	Y	N	O	M	I	A	L

Question: Problems?

Problems?

How to transmit the key?

Easy to brute force

Frequency Analysis

Frequency Analysis

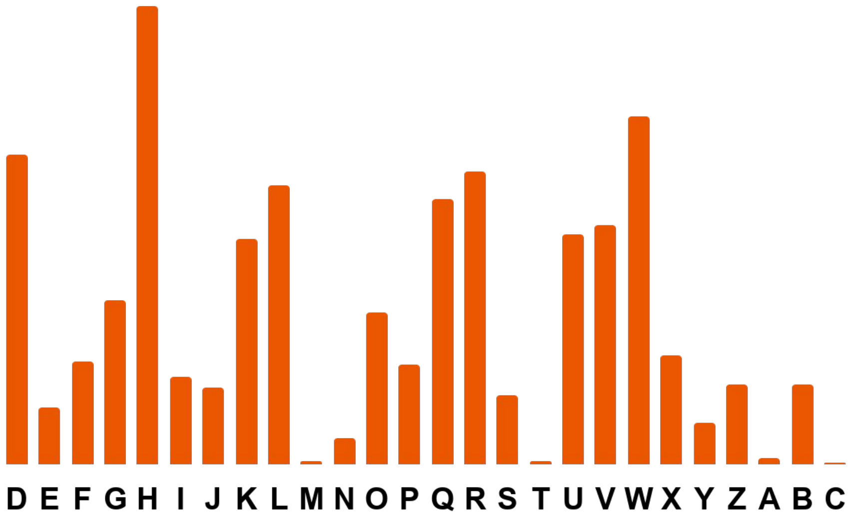
First mentioned in the 9th century by the arab polymath Al-Kindi

800 years after Caesar first used Caesar Cipher

Uses the relative frequencies of letters to determine by how many letters the message was shifted

Regular Alphabet

After Caesar Shift



Caesar Cipher Conclusion

Easy way to encrypt a message

Has some fatal flaws

Was likely still considered secure during its time

RSA

Rivest

Shamir

Adleman

RSA

RSA is one of the most used encryption systems

Used in:

SSL/HTTPS

SSH

Bitcoin

PGP or GPG

RSA is asymmetric

Two keys: public (to encrypt) and private (to decrypt)

Solves key transmission problem

RSA Encryption

RSA encryption uses multiple mathematical steps

A very significant one is multiplication with a very large number

That number has certain properties: it is the product of two primes

RSA-129:
1143816257578888676692357799761466120
1021829672124236256256184293570693524
5733897830597123563958705058989075147
599290026879543541

RSA Decryption

To decrypt the message you then need the two prime factors of that number

What makes RSA secure is that those prime factors are very difficult to determine

RSA-129 =
3490529510847650949147849619903898133
417764638493387843990820577
·
32769132993266709549961988190834461413
177642967992942539798288533

How safe is RSA really?

RSA-129 Challenge started in 1977

Finally beaten in 1994 using far better hardware and algorithms

How safe is RSA really?

Advances in processing power are somewhat predictable

Advances in algorithms however, are not

Caesar Cipher was vulnerable to Frequency analysis

How can we be sure that there are no critical vulnerabilities in RSA?

Possible Vulnerability

One method using polynomials could pose a threat to RSA

Possible Vulnerability in RSA Encryption

Every number can be represented as a polynomial

There are efficient algorithms to factor polynomials

From those it is possible to deduct the prime factors of the original Number

$15 = 1111 = 2^3 + 2^2 + 2^1 + 2^0 = 8 + 4 + 2 + 1$

$15 = 1111 = 2^3 + 2^2 + 2^1 + 2^0 = 8 + 4 + 2 + 1$

Substitute x for 2: $x^3 + x^2 + x^1 + x^0$

$15 = 1111 = 2^3 + 2^2 + 2^1 + 2^0 = 8 + 4 + 2 + 1$

Substitute x for 2: $x^3 + x^2 + x^1 + x^0$

$x^3 + x^2 + x^1 + x^0 \triangleq 2^3 + 2^2 + 2^1 + 2^0 \triangleq 15$

$15 = 1111 = 2^3 + 2^2 + 2^1 + 2^0 = 8 + 4 + 2 + 1$

Substitute x for 2: $x^3 + x^2 + x^1 + x^0$

$x^3 + x^2 + x^1 + x^0 \triangleq 2^3 + 2^2 + 2^1 + 2^0 \triangleq 15$

$x^3 + x^2 + x^1 + x^0 = x^3 + x^2 + x + 1 = (x^2 + 1) \cdot (x + 1)$

$15 = 1111 = 2^3 + 2^2 + 2^1 + 2^0 = 8 + 4 + 2 + 1$

Substitute x for 2: $x^3 + x^2 + x^1 + x^0$

$x^3 + x^2 + x^1 + x^0 \triangleq 2^3 + 2^2 + 2^1 + 2^0 \triangleq 15$

$x^3 + x^2 + x^1 + x^0 = x^3 + x^2 + x + 1 = (x^2 + 1) \cdot (x + 1)$

$(2^2 + 1) \cdot (2 + 1) = 5 \cdot 3 = 15$

Result: The Prime Factors of 15 are 5 and 3

However: This new process does not threaten RSA Encryption

This is shown by a new proof by Breuillard and Varjú

Why is That?

Not every factorizable number corresponds to a reducible polynomial

Example: $25 = 2^4 + 2^3 + 1$

But: $x^4 + x^3 + 1$ is irreducible

Amount of Prime Numbers and Prime Polynomials

Mathematicians have long suspected that polynomials are much more likely to be irreducible the larger they get

Amount of Prime Numbers

1 **2** **3** 4 **5** 6 **7** 8 9 10 **11** 12 **13** 14 15 16 **17** 18 **19** 20 21 22 **23** 24 25 26 **27** 28 **29** 30

Potential divisors for 7: 2, 3, 5

Potential divisors for 27: 2, 3, 5, 7, 11, 13, 17, 19, 23, 27, 29

Larger numbers are less likely to be prime numbers

Polynomials are Different

A polynomial can only be factorized if its coefficients are in the correct ratio to one another.

Example:

$x^2 + 5x + 6 = (x + 3) \cdot (x + 2)$

Polynomials are Different

A polynomial can only be factorized if its coefficients are in the correct ratio to one another.

Example:

$x^2 + 5x + 6 = (x + 3) \cdot (x + 2)$

Because:

$2 + 3 = 5$

$2 \cdot 3 = 6$

Polynomials are Different

More complex polynomials lead to more such conditions.

The more conditions there are, the less likely it is to find a reducible polynomial.

And for RSA?

Larger Polynomials are more likely to be irreducible

The numbers used in RSA would turn into giant polynomials

It is very unlikely that those polynomials are reducible

RSA-129 as a Polynomial

RSA-129:
114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

≙

$2^{425} + 2^{423} + 2^{421} + 2^{417} + 2^{416} + 2^{415} + 2^{414} + 2^{413} +$
....

≙ (for x = 2)

$x^{425} + x^{423} + x^{421} + x^{417} + x^{416} + x^{415} + x^{414} + x^{413} +$
....

Modern RSA Key Sizes

RSA-129	426 bits	129 digits
deprecated	1024 bits	309 digits
Most recommended	2048 bits	617 digits
futureproof	4096 bits	1234 digits

Prime Polynomials and RSA Encryption

Practical Applications in Encryption

A potential weakness in RSA

...and why you shouldn’t be worried