What is the Smallest RSA Private Key

Why is there, at all, such a thing? Why is it not 42? Why is the smallest public key not 35? Or, for that matter, 6?

Shachar Shemesh Lingnu Open Source Consulting



http://creativecommons.org/licenses/by-sa/2.5/il/



Introducing the Players

Alice and Bob

- **A** Want to communicate.
- In this lecture, we'll assume Alice wants to send a message to Bob without anyone listening.

👌 Eve

- ∆ The attacker
- In our case, we'll assume she wants to intercept and understand the message sent from Alice to Bob.

Open Source Consult@ Classic Encryption
 Symmetric Key Cryptography
 Alice and Bob have a shared secret.

A Usually a totally random set of bits.

 Δ This secret is called "the key".

△ The key has to be shared via a secure channel.

If Eve learns of the key, she will be able to decipher the message.

△ Alice's and Bob's keys are the same.



Asymmetric Encryption

Alice and Bob are communicating over insecure line.
 Eve can listen in at will.

- △ Alice describes the algorithm to Bob.
- △ Bob generates a key and tells it to Alice.
- △ Alice encrypts the message and sends it to Bob.
- Eve hears the algorithm, the key and the encrypted message, and yet cannot know what Alice's message was.

Open Source Consulting Merkle's Puzzles First Algorithm of Family

A Bob encrypts 2²⁸ blocks with known P and unique I.

- A Bob sends all of the encrypted data, as well as all but 28 bits of each key, to Alice.
- Alice chooses an encrypted block at random, and invests the CPU required to brute force the missing bits from the key.
- △ Alice sends the corresponding I to Bob.
- Bob now knows which block Alice picked, and they have a shared secret.
- Eve has to brute force all blocks in order to find the right one.
 http://lingnu.com



Merkle's Puzzles Analysis

Bob has to perform 2²⁸ encryptions in order to encrypt all blocks.

- Alice has to perform around 2²⁸ (2²⁷ on average) to brute force the missing 28 bits of the key.
- A Eve has to brute force $(2^{27} \text{ on average})$ an average of half the blocks (2^{27}) in order to find the key = 2^{54} , can get as bad as 2^{56} .
- All in all, both Alice and Bob invest the square root of what Eve has to invest in order to agree on a key.



Background – What is RSA

A Named after its inventors:

👌 Ron Rivest

👌 Adi Shamir

[∆] Leonard Adleman

Description
A Public Key encryption

A Public key used for encryption

A Private key used for decryption

[∆] No easy way to get from public to private key

Mathematically Based Encryption

Unlike the Merkle's Puzzles above, Public Key encryption is based on mathematical principles.

A Two popular mathematical principles:

 Δ Discrete root – the basis for RSA

Open Source Consultina

∆ Discrete log – the basis for DSA, ElGamal and Diffie Hellman.

△ Public key keys cannot be any number.

As the algorithm is mathematical, the keys have to keep some mathematical properties.

Typically, 64 bits is an ok size for a symmetric key. An RSA key should be no less than 512 bits, 1024 as preference.



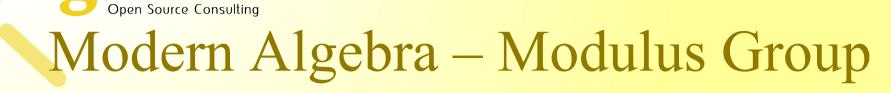
RSA Mathematical Principles

Modern algebra, here we come...

Traditional Numbers Group Traditional Algebra

[∆] A quick reminder:

- $\mathbb{A} \mathbb{N}$ Natural numbers (1, 2, 3 etc.)
- $\mathbb{A}\mathbb{Z}$ Whole numbers (\mathbb{N} + negatives and zero)
- $\bigcirc \mathbb{Q}$ Rational numbers. Any number that can be denoted as a division of two numbers from \mathbb{Z}
- $\Delta \mathbb{R}$ Real numbers.
- $\Delta \mathbb{C}$ Complex numbers.
- △ All of the above groups are infinite in size
 - $\Delta \mathbb{N}, \mathbb{Z} \text{ and } \mathbb{Q} \text{ are } \aleph_0$
 - $\Delta \mathbb{R}$ and \mathbb{C} are \aleph



- What happens if we limit ourselves to a finite sized group?
- ▲ We'll call it "all the whole numbers smaller than *n*", and mark it with \mathbb{Z}_n .
 - $\Delta E.g. \mathbb{Z}_{5}$ will be the group { 0, 1, 2, 3, 4 }
- △ Arithmetics "+" and "×" are defined as with \mathbb{Z} , taking the reminder (modulus) from *n*.
 - Δ The operation is marked accordingly with "mod *n*".
 - A We use the congruent (≡) sign instead of equal (=) 3+4=7≡2 mod 5 3×3=9≡4 mod 5



Inversing the + Operator

- ▲ Inversing the "+" operator is no more than applying the "+" semantics to "-".
- Simply perform the same operation you would on \mathbb{Z} , and then take the positive modulus *n* of the result.
 - ∆ 1–4≡2 mod 5
 - ∆ 1–4≡3 mod 6
 - ∆ 1–4≡4 mod 7



 Δ gcd(*a*,*b*) is the biggest number that divides both *a* and *b*.

d gcd(12,4)=4

Open Source Consulting

- Δ gcd(15, 12)=3
- $\Delta \gcd(15, 8) = 1$

∆ Numbers that have a gcd of 1 are called "coprime".

 Δ It means they have no common prime factors.

▲ A close relative – Least Common Multiple

 Δ For two numbers, $lcm(a,b)=a \cdot b/gcd(a,b)$

Den Source Consulting Euclid's Algorithm For Finding GCD

Δ To compute gcd(*a*,*b*) for *a*>*b*

- ∆ Compute $a=c_1 \cdot b+r_1$, where $r_1 < b$ and all numbers are whole.
- \bigtriangleup Compute $b = c_2 \cdot r_1 + r_2$
- A Repeat until r_i is zero (in other words, until r_{i-1} cleanly divides r_{i-2}).

 Δ When that happens, r_{i-1} is the gcd.



Example – gcd(21, 102)

- $102 = 4 \cdot 21 + 18$
- $21 = 1 \cdot 18 + 3$
- 18=6.3+0
- gcd(21, 102)=3





A Useful Trick

Euclid's Extended Algorithm:

Any two numbers *a* and *b* will have whole numbers *p* and *r* such that $p \cdot a + r \cdot b = \gcd(a, b)$



- $18 = 6 \cdot 3 + 0$
- gcd(21, 102)=3

3=21-1.18=21-1.(102-4.21)=5.21-1.102



Inversing the × Operator

- △ We seek "b" such that $b \times a \equiv c \mod m$.
- [∆] In particular, we would like to find the solution for $b \times a \equiv 1 \mod m$. We call *a* "the inverse of *b*", or b^{-1} .
 - \triangle Example: $5^{-1} \equiv 3 \mod 7$
 - $3 \times 5 \equiv 15 \equiv 1 \mod 7$

Open Source Consulting An Inverse Doesn't Necessarily Exists Δ Let's try to find 2⁻¹ over \mathbb{Z}_{A} : $2 \times 0 \equiv 0 \mod 4$, $2 \times 1 \equiv 2 \mod 4$, $2 \times 2 \equiv 0 \mod 4$, $2 \times 3 \equiv 2 \mod 4$ Δ On the other hand: $3 \times 3 = 9 \equiv 1 \mod 4$ Δ 3 is its own inverse mod 4. Δ In order for *a* to have an inverse in \mathbb{Z}_{p} , it must be coprime to n. In other words, a^{-1} exists IFF gcd(a,n)=1 Δ If a is coprime to n, a is also called a "generator" of \mathbb{Z}_{p} . $\Delta a \times i \mod n$ will generate all members of \mathbb{Z}_n when *i* goes from 0 to *n*-1.

How To Find an Inverse

Δ To find $a^{-1} \mod n$

Open Source Consulting

- \bigtriangleup Perform Euclid's extended algorithm to calculate gcd(*a*,*n*)
- ∆ If the result is not 1, there is no inverse.
- Δ If the result is 1, figure out *p* and *r* as before.
- Δ We now have $p \cdot a + r \cdot n = 1$
- ∆ Stated over \mathbb{Z}_n , this turns into $p \cdot a + r \cdot n \equiv 1 \mod n$.
- △ However $n \equiv 0 \mod n$ for every *n*.
- [∆] We are left with $p \cdot a + r \cdot 0 \equiv 1 \mod n$, which can also be written as $p \cdot a \equiv 1 \mod n$.
- Δ It follows that *p* is *a*'s inverse.

Example – Calculate 9⁻¹ mod 16

 $16 = 1 \cdot 9 + 7 \qquad 7 = 16 - 1 \cdot 9$

- $9 = 1 \cdot 7 + 2$
- $7 = 3 \cdot 2 + 1$
- $2 = 2 \cdot 1 + 0$
- gcd(16, 9)=1

2=9-1.7 1=7-3.2=7-3.(9-1.7) =-3.9+4.7 =-3.9+4.(16-1.9) 1=4.16-7.9

$9^{-1} = -7 \equiv 9 \mod 16$

How Many Numbers Have Inverses?

- A We denote by the function $\varphi(n)$ (Greek letter "phi") the number of numbers smaller than *n* that are coprime to it.
- $\Delta \phi$ is easy to calculate in certain cases:
 - \triangle For any prime *p* we have $\varphi(p)=p-1$

Open Source Consulting

 Δ If *a* and *b* are coprime, then $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$



Fermat's Theorem (Not That One)

- [∆] For every prime integer *p* and any *a*, we can say that $a^p \equiv a \mod p$.
- △ Put another way, $a^{p-1} \equiv 1 \mod p$
- Often called "Fermat's little theorem"
- ∆ We can also apply Euler's more general theorem:
 - $a^{\varphi(n)} \equiv 1 \mod n$
 - Δ Applies for any *n*, prime or otherwise.
 - Δa must be coprime to n.

Chinese Reminder Theorem • It is possible to find x such that: $x \equiv a_1 \mod n_1$ $x \equiv a_2 \mod n_2$ $x \equiv a_i \mod n_i$ for a known set of a_i and n_i .

The constants have to conform to a certain consistency rule.

 Δ If all *n*s are coprime in pairs, this rule is guaranteed.

 Δx will repeat every lcm $(n_1, n_2, ..., n_i)$

∧ Reminder – if all *n*s are coprime in pairs, $lcm(n_1, n_2, ..., n_i)$ is simply $n_1 \times n_2 \times ... \times n_i$ http://lingnu.com



The RSA Encryption Algorithm

And you thought this moment will never come....



Encryption

- An RSA public key is composed of two numbers:
 - Δ Encryption exponent. We'll use "*e*".
 - Δ The actual public key. We'll call it "*n*".
- ▲ To encrypt the message "*m*" into the encrypted form *M*, perform the following simple operation: $M=m^e \mod n$
- When performing the power operation, actual performance greatly depends on the number of "1" bits in *e*.
 - \triangle Originally used to use e=3.
 - Δ Today we usually use $e=2^{16}+1=65,537$



Decryption

In order to decrypt, we need to reverse the exponent used for encryption.

- [∆] We know, from Fermat's and Euler's theorems that: $m^{\varphi(n)+1} \equiv m \mod n$
- Δ We have $M \equiv m^e \mod n$
- Δ We need to find $d \equiv e^{-1} \mod \varphi(n)$
- $\Delta Decryption is merely:$ $m \equiv M^d \mod n$



Selecting the Keys

When selecting the public key n we make sure that this will be possible.

- \bigtriangleup For one thing, we need to make sure that e and $\varphi(n)$ are coprime.
- Δ In order to generate the keys we select two prime numbers. We'll call them p and q.
 - $\Delta n = p \times q$
 - $\Delta e=3$ (or 65,537, as the case may be)
 - (p-1)(q-1)

 $\Delta d = e^{-1}$ is calculated using Euclid's extended algorithm.

What's the Minimal RSA Public Key?

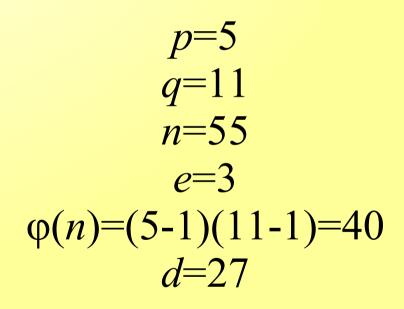
△ First attempt – smallest primes. p=2, q=3, n=6.

Open Source Consulting

- ▲ Problem cannot encrypt. φ(6)=(2-1)(3-1)=2. $3^{-1}=1 \mod 2$. In other words, to decrypt you need to raise by the power of "1". In yet other words, *e* does not encrypt. Each m is mapped to itself.
- Second attempt keep the primes bigger than *e*. p=5, q=7. n=35
 - ♦ Problem φ(35)=(5-1)(7-1)=24. gcd(*e*,φ(n))=gcd(3,24)=3. *e*⁻¹ doesn't exist.
 - ∆ Must keep gcd(e,φ(n)) by keeping e and p−1 and e and q−1 coprime.
 - & 5 was ok as private key part gcd(3,4)=1. Next prime is 11.



Found the Minimal RSA Key





Example

Using a public key of 55 and an *e* of 3 we encrypted a message $m^3 \mod 55$ and got M=3.

What was the original message?



A Little Performance Trick

- **A** When performing decryption, *p* and *q* are often known.
- Standard decryption method: $m \equiv M^d \mod n$
- A Quicker decryption method:
 - $\sum m_1 \equiv M^d \mod p$
 - $m_2 \equiv M^d \mod q$
 - Δ Use the Chinese reminder theorem to calculate $m \mod n$

Found the Minimal RSA Key

Lingnu

Open Source Consulting

$$p=5q=11n=55e=3 $\varphi(n)=(5-1)(11-1)=40$
d=27
 $d_p=d \mod p-1=27 \mod 4=3$
 $d_p=d \mod q-1=27 \mod 4=3$$$



Example Decryption

$$M=3n=55m_p \equiv 3^3 \mod 5=2m_q \equiv 3^7 \mod 11=9m \equiv 42 \mod 55$$

Encrypting Multiples of p or q

- Δ Euler's theorem only applies to numbers coprime to n.
 - We are not, at all, sure that we *can* decrypt such a message!
- Δ Let's assume m^e is an encrypted message, and that m is a multiple of p.
 - $\Delta m \equiv 0 \mod p$, therefor $m^e \equiv 0 \mod p$

Open Source Consultina

- A We know that $d≡e^{-1} \mod φ(n)$, which means $d≡e^{-1} \mod q-1$.
- So we know that raising to the power of d will do nothing mod p (zero is unaffected), and will decrypt mod q (due to Fermat's little theorem).

http://lingnu.com

∆ Hence, these message will decrypt as well.



RSA Security

 Δ In order to decrypt Alice's messages, Eve needs to figure out d.

- ▲ No (known) efficient method of obtaining *d* other than calculating e^{-1} mod φ(n)
- ▲ No (known) efficient method of calculating e^{-1} mod φ(n) without knowing φ(n).
- Δ No (known) efficient method of factorizing *n*.
- △ No (known) method for breaking RSA.

Relative Complexity of Algorithms

Complexity of operations:

Open Source Consulting

- O(gcd(a,b)) = log(min(a,b)) division operations.
- Some pretty effective probability algorithms for finding prime numbers.
- ∆ No efficient algorithm for factorizing a number.
- Eve needs to work non-polynomially harder than Alice and Bob in order to attack their keys.



Bonus Material

Decrypting Messages Without d



Alice has to send the same message to Bob, Charlie and Debbie.

A Each provided Alice with their respective public key.

 Δ Unsurprisingly, they all use the same *e* of 3.

Open Source Consulting

∧ Alice computes $m^3 \equiv M_b \mod n_b$, $m^3 \equiv M_c \mod n_c$, $m^3 \equiv M_d \mod n_d$.

▲ If Eve knows that M_{b} , M_{c} and M_{d} were generated from the same *m*, she can obtain *m* without knowing any of the required *d*s.



Attack Method

 $\Delta \text{ Eve knows:}$ $m^{3} \equiv M_{b} \mod n_{b}$ $m^{3} \equiv M_{c} \mod n_{c}$ $m^{3} \equiv M_{d} \mod n_{d}$

 \triangle Eve uses the Chinese reminder theorem to calculate m^3 .

 \triangle Eve takes the regular 3rd root of m^3 .

 Δ Eve knows m.

△ Now you know why e=3 was replaced with e=65,537.



That's All, Folks