RSA

Sasha Levinshteyn

Outline

Section 1

Public-Key Cryptosystems

General Idea

- Each user publicizes their encryption procedure E
- The user determines their corresponding decryption procedure D
- The user does not reveal D

Goal

- Alice has a message M to send to Bob
- Need an encryption method E and a decryption method D such that
  - $D(E(M)) = M = E(D(M))$
  - Both E and D are easy to compute
  - Publicly revealing E doesn't reveal D
- We want an encryption key (e, n) and a decryption key (d, n)

Section 2

RSA Algorithm

Key Distribution

- If Bob sends a message M to Alice...
- Alice sends her public encryption key (e, n) to Bob
- She keeps her private decryption key d

Encryption

- Bob turns his message M into some number $m < n$
- Long messages can be split up into chunks
- He computes the ciphertext c using the encryption algorithm E:

$$c \equiv E(m) \equiv m^e \mod n$$

- Computers would use exponentiation by repeating squaring and multiplication

Decryption

- Alice receive the ciphertext c
- She decrypts it and finds m using the decryption algorithm D:

$$m \equiv D(c) \equiv c^d \mod n$$

- How do we find a valid e, d, and n?

Key Generation

1. Choose 2 prime numbers p and q
2. Compute $n = p \cdot q$
3. Compute $\phi(n) = (p-1) \cdot (q-1)$
   - We actually use the Carmichael function now instead $\implies \lambda(n) = \text{lcm}(p-1, q-1)$
4. Choose d relatively prime to $\phi(n)$ $\implies \gcd(d, \phi(n)) = 1$
5. Choose e to be the multiplicative inverse of $d \mod \phi(n)$ $\implies e \cdot d = 1 \mod \phi(n)$
   - Computers would use Euclid's algorithm

Example

1. Choose $p = 47$ and $q = 59$
2. Compute $n = p \cdot q = 47 \cdot 59 = 2773$
3. Compute $\phi(n) = (p - 1) \cdot (q - 1) = 46 \cdot 58 = 2668$
4. Choose $d = 157$, which is relatively prime to $\phi(n) = 2668$
5. We find that $e = 17$ as $17 \cdot 157 \equiv 1 \mod 2773$
6. We release $(n, e) = (2773, 17)$ as our public key and keep $d = 157$ as our private key

Example

1. Convert the message to numbers and encrypt

$$
\begin{aligned}
&\text{ITS ALL GREEK TO ME} \\
&\implies 0920190001121200071805051100201500130500 \\
&\implies 0948234210841444266323900778077402191655
\end{aligned}
$$

2. We write the first block ($m = 920$) as

$$m^{17} \equiv 920^{17} \equiv 948 \mod 2773$$

Section 3

Proof of Correctness

Proof

- $\phi(n)$ is the Euler totient function returning the number of integers k less than n relatively prime to n
  $\implies \gcd(k, n) = 1, k < n$
- Note that for a prime number p,

$$\phi(p) = p - 1$$

- Then,

$$\begin{aligned} \phi(n) &= \phi(p) \cdot \phi(q) \\ &= (p-1) \cdot (q-1) \end{aligned}$$

More Proof

- d is relatively prime to $\phi(n) \implies d$ has a multiplicative inverse mod $\phi(n)$
- Consider $D(E(m))$ and $E(D(m))$

$$D(E(m)) \equiv (E(m))^d \equiv (m^e)^d \equiv m^{e \cdot d} \mod n$$
$$E(D(m)) \equiv (D(m))^e \equiv (m^d)^e \equiv m^{e \cdot d} \mod n$$

- Then,

$$e \cdot d \equiv 1 \mod \phi(n) \implies m^{e \cdot d} \equiv m^{k \cdot \phi(n)+1} \mod n$$

Even More Proof

- For any integer a which is relatively prime to b,

$$a^{\phi(b)} \equiv 1 \mod b.$$

- So, as $p-1$ and $q-1$ divide $\phi(n)$

$$m^{p-1} \equiv 1 \mod p \implies m^{k\cdot\phi(n)+1} = m \mod p$$
$$m^{q-1} \equiv 1 \mod q \implies m^{k\cdot\phi(n)+1} = m \mod q$$

- These equations yield that for all m (as they are trivially true for $m \equiv 0 \mod p$),

$$m^{e\cdot d} \equiv m^{k\cdot\phi(n)+1} = m \mod n$$

Security

- Security relies on the difficulty of factoring n
  - About 200 digits long and 3.8×10^9 years to factor by 1977 standards
  - Typically a few hundred digits now
  - If we were to know p and q, we could perhaps find d from e
- Computing $\phi(n)$ would allow us to find d as the multiplicative inverse of $e \mod \phi(n)$
- Finding $\phi(n)$ or determining d otherwise is at least as hard as factoring n
- If only there was some way to factor n in polynomial time...

Section 4

Conclusion

Conclusion

- RSA is very cool
- Average Passover with too much wine moment (this is supposedly how Rivest came up with this idea)

Questions?

The era of electronic mail may soon be upon us.

— Rivest, Shamir, and Adleman (1977)

[SA77]

Bibliography I

R.L. Rivest A. Shamir and L. Adleman.

A method for obtaining digital signatures and public-key cryptosystems.

https://people.csail.mit.edu/rivest/Rsapaper.pdf, 1977.

Accessed: 03-17-2024.