RSA

Ronald L. Rivest, MIT
Adi Shamir, Weizmann
Len Adleman, USC
NEC C&C Award Lecture
November 25, 2009
Outline

- Context and History
- Invention of RSA
- Impact
Context and History

- “If I have seen a little further, it is by standing on the shoulders of giants.” (Isaac Newton, 1676)
Giant #1: Gauss

- Carl Frederich Gauss (1777-1855)
- Father of modern number theory
- Disquisitiones Arithmeticae (1801)
Giant #2: Claude Shannon

Communication Theory of Secrecy Systems*

By C. E. SHANNON

A Mathematical Theory of Communication

By C. E. SHANNON
Giant(s) #3: H, S, B, C, K

- Algorithms and Complexity Theory
- Cryptography needs:
  - *easy problems* (such as multiplication or prime-finding, for the “good guys”) and
  - *hard problems* (such as factorization, to defeat an adversary).
Invention of Public-Key Crypto

- Diffie and Hellman published “New Directions in Cryptography” Nov ’76: “We stand today at the brink of a revolution in cryptography.”
- Proposed “Public-Key Cryptosystem”. (This remarkable idea developed jointly with Merkle.)
- Introduced even more remarkable notion of **digital signatures**.
The challenge

- Diffie and Hellman left open the problem of realizing a PKC: finding $E$ and $D$ s.t.

$$D(E(M)) = E(D(M)) = M$$

where $E$ is public, $D$ is private.
- At times, we thought it impossible...
- Since then, we have learned "Meta-theorem of Cryptography": Any apparently contradictory set of requirements can be met using right mathematical approach...
S, R, and A in '78
Invention of RSA

- Tried and discarded many approaches, including some “knapsack-based” ones. (Len was great at killing off bad ideas.)
- “Group of unknown size” seemed useful idea... as did “permutation polynomials”...
- After a “seder” at a student’s...
- “RSA” uses $n = pq$ product of primes:

$$C = M^e \pmod{n} \quad \text{[public key (e,n)]}$$
$$M = C^d \pmod{n} \quad \text{[private key (d,n)]}$$
TM-82 4/77; CACM 2/78

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

Ronald Rivest, Adi Shamir, Len Adleman

April 1977

A method is presented with the novel property that publicly revealing an encryption key does not directly reveal the corresponding decryption key. This has two important consequences:

1. Certain or other secret uses are not needed to transmit keys, since a message can be encrypted using an encryption key publicly revealed by the intended recipient. Only he can decipher the message since only he knows the corresponding decryption key.

2. A message can be "signed" using a privately held decryption key. Anyone can verify the signature using the corresponding publicly revealed encryption key. This has obvious applications to "digital mail" and "electronic funds transfer" problems. A message is encrypted by representing it in a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product N of two large prime numbers p and q. Encryption is said to be a different, secret, power d. The verification of the secret message is equivalent to raising the encrypted message to the secret power d and then taking the remainder when divided by N. The security of the system seems to depend on the difficulty of the problem of finding the secret power d given the public power e, the two large prime numbers p and q, and the product N.

The encryption procedure can be made more secure by making e and d very large numbers. An experiment in which 100 messages were transmitted using a 129-digit encryption key and a 159-digit decryption key showed that it was not practical to determine the message even if the method of encryption was known. The experiment also showed that the encryption key could be used to encrypt messages without being able to decrypt them.

Keywords and Phrases: digital signature, public-key cryptosystems, primes, certification authority, security, hashing, knapsack, lattices, knapsack, electronic funds transfer, cryptography.

A method is presented for obtaining digital signatures and public-key cryptosystems using a novel property that publicly revealing an encryption key does not directly reveal the corresponding decryption key. This has two important consequences:

1. Certain or other secret uses are not needed to transmit keys, since a message can be encrypted using an encryption key publicly revealed by the intended recipient. Only he can decipher the message since only he knows the corresponding decryption key.

2. A message can be "signed" using a privately held decryption key. Anyone can verify the signature using the corresponding publicly revealed encryption key. This has obvious applications to "digital mail" and "electronic funds transfer" problems. A message is encrypted by representing it in a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product N of two large prime numbers p and q. Encryption is said to be a different, secret, power d. The verification of the secret message is equivalent to raising the encrypted message to the secret power d and then taking the remainder when divided by N. The security of the system seems to depend on the difficulty of the problem of finding the secret power d given the public power e, the two large prime numbers p and q, and the product N.

The encryption procedure can be made more secure by making e and d very large numbers. An experiment in which 100 messages were transmitted using a 129-digit encryption key and a 159-digit decryption key showed that it was not practical to determine the message even if the method of encryption was known. The experiment also showed that the encryption key could be used to encrypt messages without being able to decrypt them.

Keywords and Phrases: digital signature, public-key cryptosystems, primes, certification authority, security, hashing, knapsack, lattices, knapsack, electronic funds transfer, cryptography.

A method is presented for obtaining digital signatures and public-key cryptosystems using a novel property that publicly revealing an encryption key does not directly reveal the corresponding decryption key. This has two important consequences:

1. Certain or other secret uses are not needed to transmit keys, since a message can be encrypted using an encryption key publicly revealed by the intended recipient. Only he can decipher the message since only he knows the corresponding decryption key.

2. A message can be "signed" using a privately held decryption key. Anyone can verify the signature using the corresponding publicly revealed encryption key. This has obvious applications to "digital mail" and "electronic funds transfer" problems. A message is encrypted by representing it in a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product N of two large prime numbers p and q. Encryption is said to be a different, secret, power d. The verification of the secret message is equivalent to raising the encrypted message to the secret power d and then taking the remainder when divided by N. The security of the system seems to depend on the difficulty of the problem of finding the secret power d given the public power e, the two large prime numbers p and q, and the product N.

The encryption procedure can be made more secure by making e and d very large numbers. An experiment in which 100 messages were transmitted using a 129-digit encryption key and a 159-digit decryption key showed that it was not practical to determine the message even if the method of encryption was known. The experiment also showed that the encryption key could be used to encrypt messages without being able to decrypt them.

Keywords and Phrases: digital signature, public-key cryptosystems, primes, certification authority, security, hashing, knapsack, lattices, knapsack, electronic funds transfer, cryptography.
Security of RSA

- Security of RSA depends on difficulty of factoring $n$ (i.e., finding $p$ and $q$)
- Difficulty appears to grow quickly as length of $n$ increases...
- But how fast does difficulty grow?
$100 RSA SciAm Challenge

- Martin Gardner publishes *Scientific American* column about RSA in August '77, including our $100 challenge (129 digit n) and our infamous “40 quadrillion years” estimate required to factor RSA-129:

114,381,625,757,888,867,669,235,779,976,146,612,010,218,296,721,242,362,562,561,842,935,706,935,245,733,897,830,597,123,563,958,705,058,989,075,147,599,290,026,879,543,541

(129 digits)

or to decode encrypted message.
$100 RSA Challenge Met '94

- RSA-129 was factored in 1994, using thousands of computers on Internet. “The magic words are squeamish ossifrage.”
- Cheapest purchase of computing time ever!
- Gives credibility to difficulty of factoring, and helps establish key sizes needed for security.
Number Theory benefits

- Hardy: ``Nothing I have ever done is of the slightest practical use."
- Research in number theory and factoring has grown, due to its relevance to cryptography and its practical implications!
Factoring milestones

- '84: 69 digits (Sandia; Time magazine)
- '91: 100 digits (Quadratic sieve)
- '94: 129 digits ($100 challenge number)
- '99: 155 digits (Number field sieve)
- '05: 200 digits (Number field sieve)
Factoring milestones

- '84: 69 digits (Sandia; Time magazine)
- '91: 100 digits (Quadratic sieve)
- '94: 129 digits ($100 challenge number)
- '99: 155 digits (Number field sieve)
- '05: 200 digits (Number field sieve)
- '01: 15 = 3 * 5 (IBM quantum computer!)
Cryptography blossoms

- RSA becomes model for new cryptographic proposals:
  - meet new requirements by
  - utilizing mathematical structures
  - connected to hard computational problems.

- Field of cryptography has grown fast, with its own professional society (IACR) and dozens of conferences every year.
Business impact

- Invention of the World Wide Web (1992) and then integration of RSA cryptography into browsers helps fuel growth of e-commerce.
From Len Adleman

“"It is one of life's great pleasures to watch the world being transformed by the technological marvels born out of the last half century of advances in computation and communications. It is a more personal pleasure to have planted a small seedling and witnessed its struggles and growth during this period of transformation."
“If, in addition, someone else notices and appreciates the fruits of your labor, it is immensely satisfying.

“I thank the NEC C&C Foundation, its President Hajime Sasaki, Executive Director Hiroshi Gokan, and other distinguished members for this award.”
Thank you!

(The End)