BigData Experience Lab
Bangalore

RSA: Public Key Encryption

Pranav Maneriker

September 2, 2016

Content

Introduction

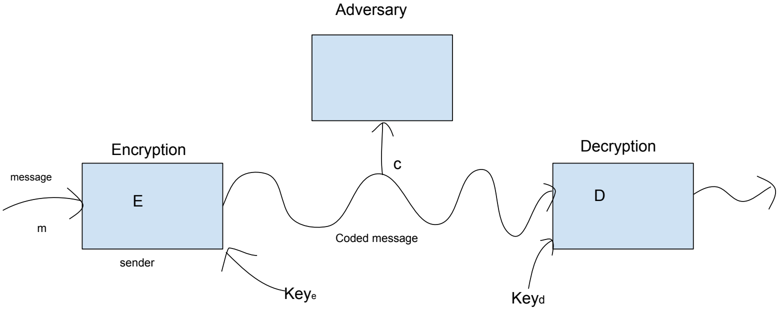

Figure: Typical Crypto Algorithm pipeline

- Chosen Plaintext
- Chosen Ciphertext
- Known Plaintext
- Known Ciphertext

Encryption

Types of Encryption

Public and Private key

- `Private key encryption`
  Shared Secret. Parties must meet and exchange key before establishing a secure communication channel.
  Examples: DES, Rijndael AES
  Fast, but tedious on their own
  Substitution Cipher demo

- `Private key encryption`
  Shared Secret. Parties must meet and exchange key before establishing a secure communication channel.
  Examples: DES, Rijndael AES
  Fast, but tedious on their own
  Substitution Cipher demo
- `Public key encryption`

Public Key Encryption

Finite Fields

We hold these truths to be self evident

- F_p^*
- Generation of a prime : **Miller Rabin Demo**
- Fermat's little theorem
- Euler Totient Theorem
- GCD algorithm, Bezout identity
- Chinese Remaindering?

Diffie-Hellman [3]
Optional

- Whitfield Diffie and Martin Hellman - Turing Award 2016
- Public key exchange protocol
- Discrete Log Problem

Sophie Germain Primes ($p = 2q + 1$)

Algorithm

- Generate a large prime p
- Fix a generator g of F_p^*
- (g, p) generated by sender/receiver and sent to other
- Sender picks random r, $0 < r < p - 1$, sends g^r to receiver
- Receiver picks a random s, $0 < s < p - 1$, sends g^s to sender
- Sender computes $(g^s)^r = g^{sr}$, Receiver computes $(g^r)^s = g^{sr}$ Shared secret key g^{sr}

RSA

- Ron Rivest, Adi Shamir, and Leonard Adleman, public description 1977
- Clifford Cocks, English mathematician, UK intelligence agency (1973), declassified 1997
- Still the most popular public key encryption

Algorithm

- Pick two large primes p and q
- Let $n = pq$
- Pick a number $e \mid 1 < e < (p-1)(q-1), gcd(e, n) = 1$
- Compute $d \mid d < (p-1)(q-1), ed \equiv 1 \mod (p-1)(q-1)$

Sender (Public Key) : (n, e)
Receiver (Private Key) : d

Sender sends m as $c = m^e \mod n$
Receiver gets c, retrieves $m = c^d \mod n$

Attacks on RSA
Simple (optional)

- Brute Force
- l-smooth prime p (choose Sophie Germain)
- Quadratic Sieve

All truths are equal, some truths are more equal than others

- Integer Lattices
- Minkowski's theorem
  For lattice $\mathbb{L} \in \mathbb{R}^m$, $\lambda(\mathbb{L}) = \sqrt{m} v(\mathbb{L})^{\frac{1}{m}}$
- Ajtai-Micciancio theorem [5]
  Given $\mathbb{L}$, finding a vector of length $\sqrt{2}\lambda(\mathbb{L})$ is NP hard
- Lenstra-Lenstra-Lovász theorem [4] (Gram-Schmidt for integer lattices)
  Can compute a vector of length $\leq 2^{\frac{n-1}{2}}\lambda(\mathbb{L})$ in polynomial time

Demo!

References

References I

[1] D. Boneh et al.
Twenty years of attacks on the rsa cryptosystem.
Notices of the AMS, 46(2):203–213, 1999.

[2] D. Coppersmith.
Finding a small root of a univariate modular equation.
In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 155–165. Springer, 1996.

[3] W. Diffie and M. Hellman.
New directions in cryptography.
IEEE transactions on Information Theory, 22(6):644–654, 1976.

[4] A. K. Lenstra, H. W. Lenstra, and L. Lovász.
Factoring polynomials with rational coefficients.
Mathematische Annalen, 261(4):515–534, 1982.

References II

[5] D. Micciancio.
The shortest vector in a lattice is hard to approximate to within some constant.
SIAM journal on Computing, 30(6):2008–2035, 2001.

[6] R. L. Rivest, A. Shamir, and L. Adleman.
A method for obtaining digital signatures and public-key cryptosystems.
Communications of the ACM, 21(2):120–126, 1978.

Thank you!