



Design and analysis of algorithms

Lecture 41 & 42

Edyta Szymańska

edyta@cc.gatech.edu

Complexity of Primes



Recent advances:

Complexity of Primes

Recent advances:

The problem of deciding whether or not an integer is a prime can be solved in time polynomial in the number of bits necessary to represent the integer at hand (that is, roughly the logarithm of the integer itself)

Complexity of Primes

Recent advances:

The problem of deciding whether or not an integer is a prime can be solved in time polynomial in the number of bits necessary to represent the integer at hand (that is, roughly the logarithm of the integer itself)

References:

*M. Agrawal, N. Kayal and N. Saxena, **PRIMES is in P***

Complexity of Primes

Recent advances:

The problem of deciding whether or not an integer is a prime can be solved in time polynomial in the number of bits necessary to represent the integer at hand (that is, roughly the logarithm of the integer itself)

References:

*M. Agrawal, N. Kayal and N. Saxena, **PRIMES is in P***

The fact that PRIME has been found to be in P cannot be used to break any cryptographic algorithms. (Moreover, the randomized algorithms are still faster.)

Cryptography

Characters:

- ⑥ Alice and Bob, who wish to communicate in private
- ⑥ Eve, an eavesdropper, who will use all her power to learn the secret between Alice and Bob

Cryptography

Characters:

- ⑥ Alice and Bob, who wish to communicate in private
- ⑥ Eve, an eavesdropper, who will use all her power to learn the secret between Alice and Bob

Cryptographic schemes:

- ⑥ the private-key scheme
- ⑥ the public-key scheme

Private-key scheme: the one-time pad



- ⑥ Alice and Bob meet beforehand and pick a random binary string r , called a *one-time pad*, $|r| = |x|$, where x is the message, which will be later sent.
- ⑥ Alice's encryption function: $e(x) = x \oplus r$
- ⑥ Bob's decryption function: $d(y) = e(y)$
- ⑥ Thus $d(e(x)) = e(x) \oplus r = x \oplus r \oplus r$.

Private-key scheme: the one-time pad

- ⑥ Alice and Bob meet beforehand and pick a random binary string r , called a *one-time pad*, $|r| = |x|$, where x is the message, which will be later sent.
- ⑥ Alice's encryption function: $e(x) = x \oplus r$
- ⑥ Bob's decryption function: $d(y) = e(y)$
- ⑥ Thus $d(e(x)) = e(x) \oplus r = x \oplus r \oplus r$.

Proposition Fix any n -bit string x , and let r be a random string. Then, over the possible choices of r , $x \oplus r$ is uniformly distributed over $\{0, 1\}^n$; that is, for any $z \in \{0, 1\}^n$, $\Pr(x \oplus r = z) = \frac{1}{2^n}$.

Private-key scheme: the one-time pad



Why *one-time pad*? - for one message only

Private-key scheme: the one-time pad



Why *one-time pad*? - for one message only

If Eve knew $x \oplus r$ and $y \oplus r$ for two messages x and y , then she could get $x \oplus y$.

Public-key cryptography

- ⑥ each person has a **public key** known to the whole world and a **secret key** known only for him/herself
- ⑥ Alice encodes the message x using Bob's public key
- ⑥ Bob uses his secret key to retrieve x .
- ⑥ Eve can see the encrypted message for Bob but is not able to decode it under certain circumstances.

Rivest-Shamir-Adelman(RSA) cryptosystem

Bob chooses his public and secret keys:

- ⑥ He picks two large (n -bit) random primes p and q .
- ⑥ Bob's public key is (N, e) , where $N = pq$ and e is a $2n$ -bit number relatively prime to $(p - 1)(q - 1)$. Commonly $e = 3$.
- ⑥ Bob's secret key is d , the inverse of e modulo $(p - 1)(q - 1)$, computed using the EXTENDED-EUCLID algorithm.

Rivest-Shamir-Adelman(RSA) cryptosystem

Alice wishes to send message x to Bob:

- ⑥ She looks up his public key (N, e) and sends him $y = (x^e \bmod N)$ computed using an efficient modular exponentiation algorithm.
- ⑥ Bob decodes the message by computing $y^d \bmod N$.

Analysis of the RSA protocol

Proposition *For any e relatively prime to $(p - 1)(q - 1)$, the mapping $x \mapsto x^e \pmod N$ is a bijection on $\{0, 1, \dots, N - 1\}$.*

Analysis of the RSA protocol

Proposition For any e relatively prime to $(p - 1)(q - 1)$, the mapping $x \mapsto x^e \pmod N$ is a bijection on $\{0, 1, \dots, N - 1\}$.

Proposition For any e relatively prime to $(p - 1)(q - 1)$, there is a corresponding d such that for all $x \in \{0, \dots, N - 1\}$, we have

$$(x^e)^d \equiv x \pmod N.$$

Analysis of the RSA protocol

Proposition For any e relatively prime to $(p - 1)(q - 1)$, the mapping $x \mapsto x^e \pmod{N}$ is a bijection on $\{0, 1, \dots, N - 1\}$.

Proposition For any e relatively prime to $(p - 1)(q - 1)$, there is a corresponding d such that for all $x \in \{0, \dots, N - 1\}$, we have

$$(x^e)^d \equiv x \pmod{N}.$$

Lemma If N is the product of two distinct primes p and q then for any z and k , $z^{k(p-1)(q-1)+1} \equiv z \pmod{N}$.

Security of the RSA protocol

Given N, e and $y = x^e \pmod N$, it is computationally intractable to determine x .

Security of the RSA protocol

Given N, e and $y = x^e \pmod N$, it is computationally intractable to determine x .

How might Eve try to guess x ?

Security of the RSA protocol

Given N, e and $y = x^e \pmod N$, it is computationally intractable to determine x .

How might Eve try to guess x ?

- ⑥ try all possible values of x (exponential time)
- ⑥ try to factor N to retrieve p and q , and then figure out d by inverting e modulo $(p - 1)(q - 1)$ (factoring is believed to be hard, to the advantage of RSA !)

Digital signatures with public keys

Alice wishes to send to Bob a digitally signed response x

Digital signatures with public keys

Alice wishes to send to Bob a digitally signed response x

- ⑥ Alice computes her **digital signature** σ for the message x using her secret key S_A and the equation $\sigma = S_A(x)$.
- ⑥ Alice sends the message/signature pair (x, σ) to Bob
- ⑥ Bob receives (x, σ) and verifies (using Alice's public key) whether $x = P_A(\sigma)$.
- ⑥ If $x = P_A(\sigma)$ then Bob concludes that x was signed by Alice.

Digital signatures with public keys

Properties:

- ⑥ digital signature is verifiable by anyone who has access to the signer's public key
- ⑥ the signed message is not encrypted
- ⑥ one can combine encryption and digital signature

Digital signatures with RSA

- ⑥ Alice creates a digital signature $\sigma = x^d \pmod N$, where x is the message and (d, N) is Alice's secret key.
- ⑥ Alice sends the pair (x, σ) to Bob
- ⑥ Bob uses Alice's public key (e, N) to verify whether the message x is recovered,
$$x = \sigma^e \pmod N = (x^d)^e \pmod N.$$