CS 252A Computing Lab-II **Autumn 2017**

Lecture 1: Cryptography

Lecturer: Sandeep K. Shukla *Scribe: Rahul Kumar*

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

1.1 Cryptography:Basic Terminology

Plaintext-text that is not computationally tagged, specially formatted, or written in code.
Encryption-It is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor.
Cyphertext-It is the encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result. The term cipher is sometimes used as a synonym for ciphertext, but it more properly means the method of encryption rather than the result.
Decryption-Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

1.2 Cryptography:Algorithms and keys

A method of encryption and decryption is called a cipher.Generally there are two related functions: one for encryption and other for decryption. Some cryptographic methods rely on the secrecy of the algorithms.All modern algorithms use a key to control encryption and decryption.Encryption key may be different from decryption key.

1.2.1 Symmetric Case

Encryption and decryption keys are the same or derivable from each other.

1.2.1.1 Issues

One big issue with using symmetric algorithms is the key exchange problem.The other main issue is the problem of trust between two parties that share a secret symmetric key. Problems of trust may be encountered when encryption is used for authentication and integrity checking. As we saw in Chapter 3, a symmetric key can be used to verify the identity of the other communicating party, but as we will now see, this requires that one party trust the other.

1.2.2 Asymmetric Case

Encryption and decryption keys are different and not derivable from each other.

1.3 DES (Data Encryption Standard)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

1.4 Public Key Cryptography

Public-key encryption is a cryptographic system that uses two keys – a public key known to everyone and a private or secret key known only to the recipient of the message. Example: When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message.

1.4.1 Public Key Cryptographic Algorithms

Find a hard math problem, that is easy to compute in the forward direction, but is difficult to solve in the reverse direction, unless you have some special knowledge.

1.5 RSA Public Keys

RSA (Rivest–Shamir–Adleman) is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem"
A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, and if the public key is large enough, only someone with knowledge of the prime numbers can decode the message feasibly.Breaking RSA [Bitcoin] encryption is known as the RSA problem. Whether it is as difficult as the factoring problem remains an open question.

1.5.1 Key Generation

The keys for the RSA algorithm are generated the following way: Choose two distinct prime numbers p and q. For security purposes, the integers p and q should be chosen at random, and should be similar in magnitude but 'differ in length by a few digits' to make factoring harder. Prime integers can be efficiently found using a primality test. Compute n = pq. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length. Compute
$\lambda(n) = lcm(\lambda(p), \lambda(q)) = lcm(p-1, q-1)$, where λ is Carmichael's totient function. This value is kept private. Choose an integer e such that $1 < e < \lambda(n)$ and gcd(e, λ(n)) = 1; i.e., e and λ(n) are coprime. Determine d as $d = e - 1(mod\lambda(n))$; i.e., d is the modular multiplicative inverse of e (modulo λ(n)).

1.5.2 Key Lengths

- The longer the key, the longer it takes to do an exhaustive key search.
- The problem space is to find the private key.
- The longer the key, the greater the computational power required to perform cryptographic operations.
- This means a trade-off between security and time/power.
- Time and power become important for portable devices

1.6 Digital Signatures

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.

1.7 Message Digest

A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula. Message digests are designed to protect the integrity of a piece of data or media to detect changes and alterations to any part of a message.

1.8 Cryptographic Hash Functions

A cryptographic hash function is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value' or 'message digest'.A hash function takes a string of any length as input and produces a fixed length string which acts as a kind of "signature" for the data provided. In this way, a person knowing the "hash value" is unable to know the original message, but only the person who knows the original message can prove the "hash value" is created from that message.

References