Midwestern State University

CMPS 4143: Programming Language Concepts

Course Notes

Professor: Griffin

Fall 2023

Last Updated: September 11, 2023

Contents

1 Introduction

1.1 Programming Language Concepts

one two three

2 Vocabulary

Tightly Coupled Loosely Coupled

- **Access control**
  A method of restricting access to resources, allowing only privileged entities access.

- **AES (Advanced Encryption Standard)**
  NIST approved standards, usually used for the next 20 to 30 years.

- **Affine Cypher**
  The affine is a type of monoalphabetic substitution cipher, where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. As such, it has the weaknesses of all substitution ciphers. Each letter is enciphered with the function (ax + b) mod 26, where b is the magnitude of the shift.

- **Algorithm (encryption)**
  A set of mathematical rules (logic) used in the processes of encryption and decryption.

- **Algorithm (hash)**
  A set of mathematical rules (logic) used in the processes of message digest creation and key/signature generation.

- **Anonymity**
  Of unknown or undeclared origin or authorship, concealing an entity's identification.

- **Asymmetric keys**
  A separate but integrated user key-pair, comprised of one public key and one private key. Each key is one way, meaning that a key used to encrypt information can not be used to decrypt the same data.

- **Authentication**
  To prove genuine by corroboration of the identity of an entity.

- **Block cipher**
  A symmetric cipher operating on blocks of plain text and cipher text, usually 64 bits.

- **Blowfish**
  A 64-bit block symmetric cipher consisting of key expansion and data encryption. A fast, simple, and compact algorithm in the public domain written by Bruce Schneier.

- **Cipher Text**
  The result of manipulating either characters or bits via substitution, transposition, or both.

- **Clear Text** (Plain Text)
  Usually refers to data that is transmitted or stored unencrypted (′ in clear ′)

- **Coprime Integers**
  In number theory, two integers a and b are said to be relatively prime, mutually prime,[1] or coprime (also written co-prime) if the only positive integer (factor) that divides both of them is 1. Consequently, any prime number that divides one of a or b does not divide the other. This is equivalent to their greatest common divisor (gcd) being 1.

- **Credentials**
  Something that provides a basis for credit or confidence.

- **Cryptanalysis**
  The art or science of transferring cipher text into plain text without initial knowledge of the key used to encrypt the plain text.

- **Cryptographic hash function**
  A cryptographic hash function (CHF) is a mathematical algorithm that maps data of arbitrary size (often called the "message") to a bit array of a fixed size (the "hash value", "hash", or "message digest"). It is a one-way function, that is, a function which is practically infeasible to invert. Ideally, the only way to find a message that produces a given hash is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes. Cryptographic hash functions are a basic tool of modern cryptography.

- **Cryptography**
  The art and science of creating messages that have some combination of being private, signed, unmodified with non-repudiation.

- **Cryptosystem**
  A system comprised of cryptographic algorithms, all possible plain text, cipher text, and keys.

- **Data integrity**
  A method of ensuring information has not been altered by unauthorized or unknown means.

- **Decryption**
  The process of turning cipher text back into plain text. DES (Data Encryption Standard) A 64-bit block cipher, symmetric algorithm also known as Data Encryption Algorithm (DEA) by ANSI and DEA-1 by ISO. Widely used for over 20 years, adopted in 1976 as FIPS 46.

- **Dictionary Attack**
  A calculated brute force attack to reveal a password by trying obvious and logical combinations of words.

- **Diffie-Hellman**
  The first public key algorithm, invented in 1976, using discrete logarithms in a finite field.

- **Discrete logarithm**
  The underlying mathematical problem used in/by asymmetric algorithms, like Diffie-Hellman and Elliptic Curve. It is the inverse problem of modular exponentiation, which is a one-way function.

- **Digital signature**
  An electronic identification of a person or thing created by using a public key algorithm. Intended to verify to a recipient the integrity of data and identity of the sender of the data.

- **Encryption**
  The process of disguising a message in such a way as to hide its substance.

- **Entropy**
  A mathematical measurement of the amount of uncertainty or randomness.

- **Fingerprint**
  A unique identifier for a key that is obtained by hashing specific portions of the key data.

- **Hash function**
  A one-way hash function—a function that produces a message digest that cannot be reversed to produced the original.

- **Integrity**
  Assurance that data is not modified (by unauthorized persons) during storage or transmittal.

- **Key**
  A means of gaining or preventing access, possession, or control represented by any one of a large number of values.

- **Key exchange**
  A scheme for two or more nodes to transfer a secret session key across an unsecured channel.

- **Key length**
  The number of bits representing the key size; the longer the key, the stronger it is.

- **Key management**
  The process and procedure for safely storing and distributing accurate cryptographic keys; the overall process of generating and distributing cryptographic key to authorized recipients in a secure manner.

- **Key splitting**
  A process for dividing portions of a single key between multiple parties, none having the ability to reconstruct the whole key.

- **MD5 (Message Digest 5)**
  Improved, more complex version of MD4, but still a 128-bit, one-way hash function.

- **Message digest**
  A number that is derived from a message. Change a single character in the message and the message will have a different message digest.

- **One-time pad**
  A large non-repeating set of truly random key letters used for encryption, considered the only perfect encryption scheme, invented by Major J. Mauborgne and G. Vernam in 1917.

- **One-way hash**
  A function of a variable string to create a fixed length value representing the original pre-image, also called message digest, fingerprint, message integrity check

- **Passphrase**
  An easy-to-remember phrase used for better security than a single password; key crunching converts it into a random key.

- **Password**
  A sequence of characters or a word that a subject submits to a system for purposes of authentication, validation, or verification.

- **Perfect forward secrecy**
  A cryptosystem in which the cipher text yields no possible information about the plain text, except possibly the length.

- **Pretty Good Privacy (PGP)**
  An application and protocol (RFC 1991) for secure e-mail and file encryption developed by Phil R. Zimmermann. Originally published as Freeware, the source code has always been available for public scrutiny. PGP uses a variety of algorithms, like IDEA, RSA, DSA, MD5, SHA-1 for providing encryption, authentication, message integrity, and key management. PGP is based on the "Web-of-Trust" model and has worldwide deployment.

- **Plain Text** (Clear Text)
  The human readable data or message before it is encrypted.

- **Polyalphabetic cipher**
  A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case. The Enigma machine is more complex but is still fundamentally a polyalphabetic substitution cipher.

- **Pseudo-Random Number**
  A number that results from applying randomizing algorithms to input derived from the computing environment, for example, mouse coordinates.

- **Private Key**
  The privately held "secret" component of an integrated asymmetric key pair, often referred to as the decryption key.

- **Public Key**// The publicly available component of an integrated asymmetric key pair often referred to as the encryption key.

- **Random Number**
  An important aspect to many cryptosystems, and a necessary element in generating a unique key(s) that are unpredictable to an adversary. True random numbers are usually derived from analog sources, and usually involve the use of special hardware.

- **Rijndael**
  A block cipher designed by Joan Daemen and Vincent Rijmen, chosen as the new Advanced Encryption Standard (AES). It is considered to be both faster and smaller than its competitors. The key size and block size can be 128-bit, 192-bit, or 256-bit in size and either can be increased by increments of 32 bits.

- **ROT-13 (Rotation Cipher)**
  A simple substitution (Caesar) cipher, rotating each 26 letters 13 places.

- **RSA**
  Short for RSA Data Security, Inc.; or referring to the principals - Ron Rivest, Adi Shamir, and Len Adleman; or referring to the algorithm they invented. The RSA algorithm is used in

public key cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.

- **Salt**
  A random string that is concatenated with passwords (or random numbers) before being operated on by a one-way function. This concatenation effectively lengthens and obscures the password, making the cipher text less susceptible to dictionary attacks.

- **Secret key**
  Either the "private key" in public key (asymmetric) algorithms or the "session key" in symmetric algorithms.

- **Session key**
  The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key is used for each communication session.

- **SHA-1 (Secure Hash Algorithm)**
  The 1994 revision to SHA, developed by NIST, (FIPS 180-1) used with DSS produces a 160-bit hash, similar to MD4, which is very popular and is widely implemented.

- **Single Sign-on**
  One log-on provides access to all resources of the network.

- **SSL (Secure Socket Layer)**
  Developed by Netscape to provide security and privacy over the Internet. Supports server and client authentication and maintains the security and integrity of the transmission channel. Operates at the transport layer and mimics the "sockets library," allowing it to be application independent. Encrypts the entire communication channel and does not support digital signatures at the message level.

- **Stream cipher**
  A class of symmetric key encryption where transformation can be changed for each symbol of plain text being encrypted, useful for equipment with little memory to buffer data.

- **Substitution cipher**
  In cryptography, a substitution cipher is a method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution.[**wiki:subcipher**]

- **Symmetric algorithm**
  Also known as conventional, secret key, and single key algorithms; the encryption and decryption key are either the same or can be calculated from one another. Two sub-categories exist: Block and Stream.

- **Timestamping**
  Recording the time of creation or existence of information.

- **Transposition Cipher**
  The plain text remains the same but the order of the characters is transposed.

- **Trust**
  A firm belief or confidence in the honesty, integrity, justice, and/or reliability of a person, company, or other entity.
- **Twofish**
  A new 256-bit block cipher, symmetric algorithm. Twofish was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the Advanced Encryption Standard (AES).
- **Validation**
  A means to provide timeliness of authorization to use or manipulate information or resources.
- **Verification**
  To authenticate, confirm, or establish accuracy.
- **XOR**
  Exclusive-or operation; a mathematical way to represent differences.