Cryptography

• Cryptography is the study of encryption and decryption schemes.
  – Used to uphold the security principles of confidentiality and integrity
Symmetric-key cryptography terms

• Also know as secret-key or single-key cryptography
• **Plaintext** – It is the original message or data
• **Encryption algorithm** – It scrambles the message by performing substitutions and transformations on the plaintext based upon a key. The output of the encryption algorithm is called ciphertext.
• **Ciphertext** – It is the scrambled version of the plaintext that the encryption algorithm produces.
• **Key** – It determines the particular type of transformations and substitutions performed by the encryption algorithm. A different key produces a different ciphertext. The key must be kept secret. The key is usually a bit string representing a number. If the algorithm is secure/good, the bigger the length of the key the more secure the data is.
• **Decryption algorithm** – It is the algorithm that unscrambles the ciphertext to the original plaintext given the correct key.

http://rfidsecurity.uark.edu
Symmetric-key Cryptography

\[ c = E(k, p) \]
\[ p = D(k, c) \]
Exclusive-OR (XOR) Cryptography
Block vs. Stream Ciphers

• **Block cipher** – It is an encryption/decryption algorithm in which data is processed in blocks. A block of plaintext produces an equal-length block of ciphertext.

• **Stream cipher** – It is an encryption/decryption algorithm in which the data is processed one bit or byte at a time.
Examples of block ciphers

• Data encryption standard (DES)
  – 1977
  – NIST
  – 64-bit blocks
  – 56-bit key
  – Too small for many applications today

• Triple DES (3DES)
  – Apply DES three times
  – Two-key version (2x56 = 112-bit key)
  – Three-key version (3x56 = 168-bit key)

• Advanced encryption standard (AES)
  – NIST Standard in 2001 after contest
  – 128-bit block size
  – Key sizes: 128-, 192-, or 256-bit key
  – Larger block size more efficient and secure
  – High throughput (fast)
  – Efficient

http://rfidsecurity.uark.edu
Stream cipher

http://rfidsecurity.uark.edu
RC4 stream cipher

• Variable key: 1-256 bytes
• Uses
  – Secure sockets layer (SSL)
  – Transport layer security (TLS)
  – Wired equivalent privacy (WEP)
  – WiFi protected access (WPA)
Asymmetric-key cryptography

• Two different related keys
  – Public key for encryption
  – Private key for decryption
• Based on functions that are easy to calculate one way but computationally difficult to calculate the other way.
• Two problems are solved
  – Key distribution
  – Digital signatures
Asymmetric key generation

- Large random number
- Key generation function
  - public key
  - private key

http://rfidsecurity.uark.edu
Asymmetric-key Cryptography
Alice encrypts message for Bob

Alice
Bob

Bob's public key
kpub__b

Bob's private key
kpriv__b

Plaintext
p

ciphertext
c

Plaintext
p

c = E ( kpub__b, p)
p = D ( kpriv__b, c)

http://rfidsecurity.uark.edu
Asymmetric-key cryptography examples

• RSA
  – 1024-, and 2048-bit keys are common
  – Cannot compare length of keys directly to symmetric cryptography key lengths

• Elliptic curve cryptography (ECC)
  – For the same key length, ECC is more secure than RSA
Hash function

- Hash function – It accepts a variable-length message and outputs a hash value (hash code, message digest)

\[ h = H(m) \]

http://rfidsecurity.uark.edu
Hash function examples

• MD5
  – Produces 128-bit hash value

• Secure hash algorithm (SHA-1)
  – 160-bit hash value

• SHA-256, SHA-384, SHA-512
  – Created after AES
Hash function threat

• An attacker can substitute file and recalculate the hash value of the new file.
Message authentication code (MAC)

• Also called a cryptographic checksum
• The MAC is a function of the message and a secret key shared between the sender and receiver to authenticate the sender to the receiver
• An attacker cannot create the correct MAC because he does not know the secret key.

http://rfidsecurity.uark.edu
MAC calculation by sender

\[ \text{mac} = \text{MAC}(k, m) \]
MAC verification by receiver

Receiver

Key

k

m||mac

split

m

MAC

mac calculated

Match?

mac received

mac = MAC ( k, m)
MAC examples

• Use a block cipher
• HMAC
  – Use standard hash function
  – key
Digital signature

• Requirements
  – Verify author, date, time of signature
  – Authenticate the message
  – Verifiable by a third party to resolve disputes

• Examples
  – Any asymmetric-key cryptography like RSA or ECC
  – Digital signature algorithm (DSA)
Asymmetric-key Cryptography for Digital Signature
Alice signs message and Bob verifies it

http://rfidsecurity.uark.edu
Authentication protocol terms

• **Authentication** – It is the process of determining if an entity, whether an individual or an object, is who/what they claim to be. Some evidence has to be provided to prove the claim such as what they know, what they have, or what they are. Passwords are the most common form of authentication and are an example of what a user knows.

• **Protocols** – Protocols define the series of messages exchanged between two or more entities and their meaning.

• **Mutual authentication protocol** – It permits parties to verify each other’s identity. This is important before exchanging keys or data.

http://rfidsecurity.uark.edu
Authentication protocol threat

• Replay attack

http://rfidsecurity.uark.edu
Asymmetric-key cryptography to establish a session key (simple authentication protocol)

(1) \( \text{kpub}_a || \text{ID}_a \)

Alice

Bob

(2) \( \text{E} (\text{kpub}_a, \text{k_session}) \)
Contact Information

Dale R. Thompson, Ph.D., P.E.
Associate Professor
Computer Science and Computer Engineering Dept.
JBHT – CSCE 504
1 University of Arkansas
Fayetteville, Arkansas 72701-1201

Phone: +1 (479) 575-5090
FAX: +1 (479) 575-5339
E-mail: d.r.thompson@ieee.org
WWW: http://comp.uark.edu/~drt/

http://rfidsecurity.uark.edu
Copyright Notice, Acknowledgment, and Liability Release

• Copyright Notice
  – This material is Copyright © 2008 by Dale R. Thompson. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or incorporated in commercial documents without the written permission of the copyright holder.

• Acknowledgment
  – These materials were developed through a grant from the National Science Foundation at the University of Arkansas. Any opinions, findings, and recommendations or conclusions expressed in these materials are those of the author(s) and do not necessarily reflect those of the National Science Foundation or the University of Arkansas.

• Liability Release
  – The curriculum activities and lessons have been designed to be safe and engaging learning experiences and have been field-tested with university students. However, due to the numerous variables that exist, the author(s) does not assume any liability for the use of this product. These curriculum activities and lessons are provided as is without any express or implied warranty. The user is responsible and liable for following all stated and generally accepted safety guidelines and practices.