University of Massachusetts Amherst

Lecture 11–Information Security

ECE 197SA – Systems Appreciation

Security in ECE Systems

- Information security
  - Information can be very valuable
  - Secure communication important to protect information
- Today's lecture:
  - Definition of security
  - Cryptographic operations
  - Security in network protocols
    - » Verifying identity in the Internet

The Value of Information

- What information would you like to protect?

What is Security?

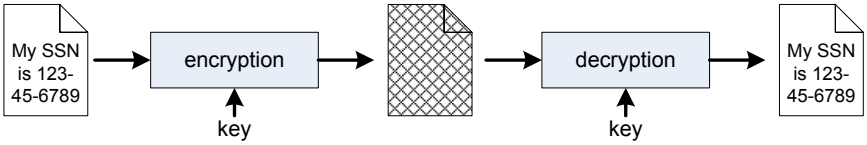
- Focus on information security
  - Security in physical world is different, but related
- What are possible attacks?

Security Properties

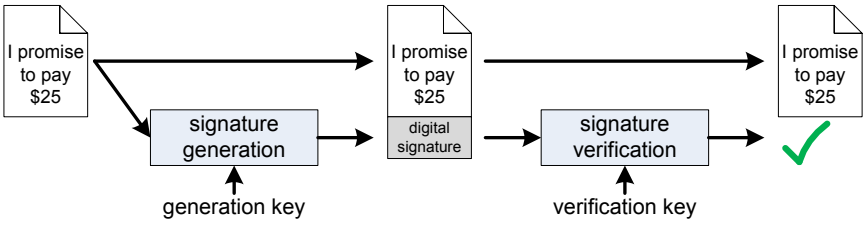
- Important properties
  - Confidentiality: information not visible
  - Authentication: information comes from known source
  - Integrity: information not modified
  - Non-repudiation: source cannot deny information
  - Availability: information is accessible
- Security models
  - CIA triad: confidentiality, integrity, availability
  - CIA + AAA: triad plus authentication, authorization, auditing
- How can these properties be achieved?

Protection Techniques

- Cryptographic algorithms

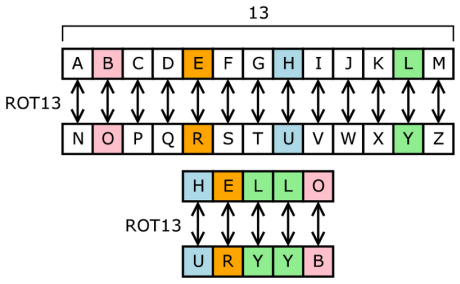


- Digital signatures



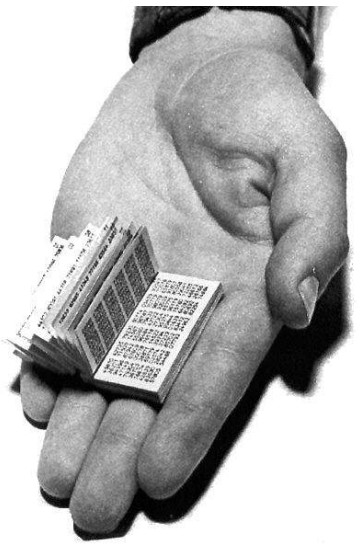
Cryptographic Algorithms

- Goal: confidential representation of information
  - Terminology: "cleartext" is encrypted into "ciphertext"
- Example: substitution
  - Key: map each letter to another letter
  - Encryption: substitute each letter
  - Decryption: reverse
  - Pros: extremely simple to implement
  - Cons: very easy to break with statistical analysis



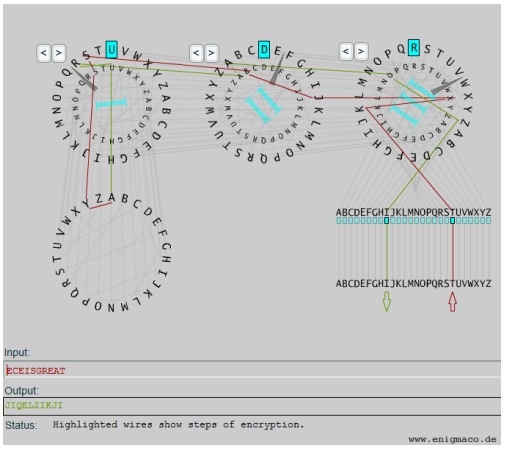
Cryptographic Algorithms

- Example: one-time pad
  - Key: truly random bit sequence
  - Encryption: XOR each bit in cleartext with one bit of key
  - Decryption: reverse
  - Pros: theoretically and practically unbreakable
  - Cons: very difficult and expensive to implement
- Need more practical approach
  - Algorithm should provide "pseudo-randomness"



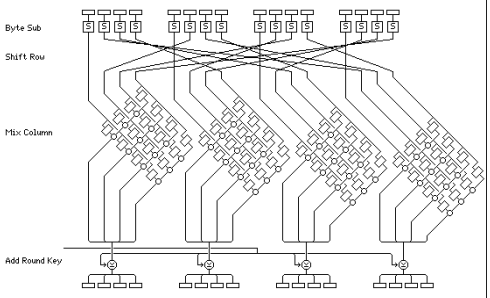
Cryptographic Algorithms

- Encoded sequence should look random
- Example: Enigma
  - Electro-mechanical rotors



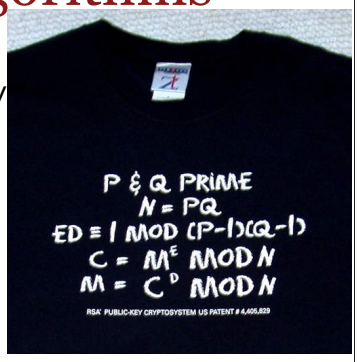
Cryptographic Algorithms

- Example: Advanced Encryption Standard (AES)
  - Key: 128, 192, or 256 bits
  - Encryption:
    - » Block cipher (128-bit blocks)
    - » 9, 11, or 13 rounds of non-linear substitutions, shifting, mixing, and use of round-specific key
  - Decryption: repeat same operations as encryption ("symmetric algorithm")
  - Pros: provides strong protection
  - Cons: parties need to share common key
  - Federal standard since 2002 (effectively replaces DES)



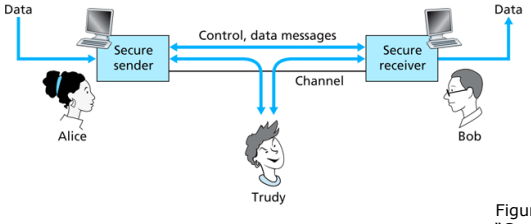
Cryptographic Algorithms

- Example: RSA encryption
  - Two keys: public key and private key
  - Asymmetric encryption/decryption
    - » Message encrypted with one key can only be decrypted with other key
  - Pros: provides unique functionality, cryptographically strong
  - Cons: very slow
  - Example use scenarios:
    - » Confidentiality: A encrypts message to B with B's public key. Only B can decrypt with its private key.
    - » Authenticity and non-repudiation: A computes hash over message, encrypts hash with its private key, and appends. B computes hash over received message, decrypts appended hash with A's public key, and compares hashes.



Security in Network Protocols

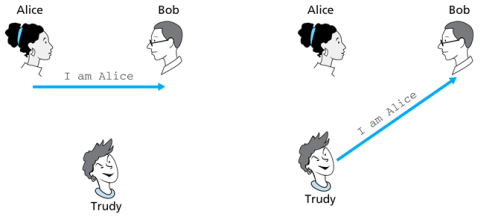
- Protocol specifies interactions (see last lecture)
- Attack model
  - Attacker can interact with protocol messages
    - » Eavesdrop
    - » Modify
    - » Insert
    - » Delete
  - Secure protocols need to be robust



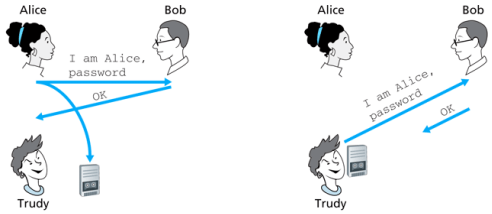
Figures from Kurose & Ross "Computer Networks"

Authentication Protocol

- Example for authentication protocol and attacks
  - Simple identifier:



  - Password:



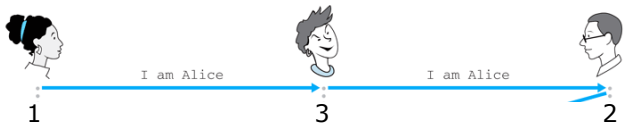
- Replay attack is a problem

Design Authentication Protocol

- Come up with protocol to authenticate message
  - Receiver should be sure that message is from real sender
    - » E.g., "I am your ECE 197SA professor. There is no class today."
  - Message is not confidential
    - » For simplicity, think of message as one entity (e.g., number)
- Process
  - Form a group of 3
  - Think about protocol
    - » Use any technique you like
  - Write down protocol
  - Try it out
    - » Person 1 authenticates themselves (incl. msg.) to person 2
    - » Person 3 checks that communication is according to protocol

Design Authentication Protocol

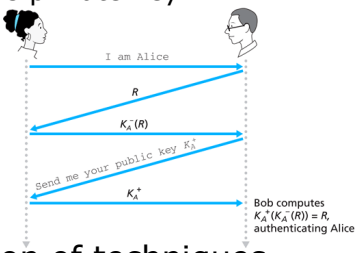
- Test your protocol under attack
  - Person 1 sends message to person 2
  - Person 3 is "in the middle"
    - » Relays, changes, replays messages



    - » Person 3 attempts to cause problems
  - Goal: avoid replay and/or change of message
    - » Your protocol should only succeed with correct message
    - » Failure is ok if person 3 violates protocol
  - Does your protocol work?
    - » Do you need to make updates to your protocol?

Secure Protocol

- Privacy
  - Encrypt with receiver's public key
- Authenticity
  - Sign hash of message with sender's private key
- Avoiding of replay
  - Use of "nonce" (random number)
  - Sender must encrypt nonce with their private key
  - Replay fails because nonce is different



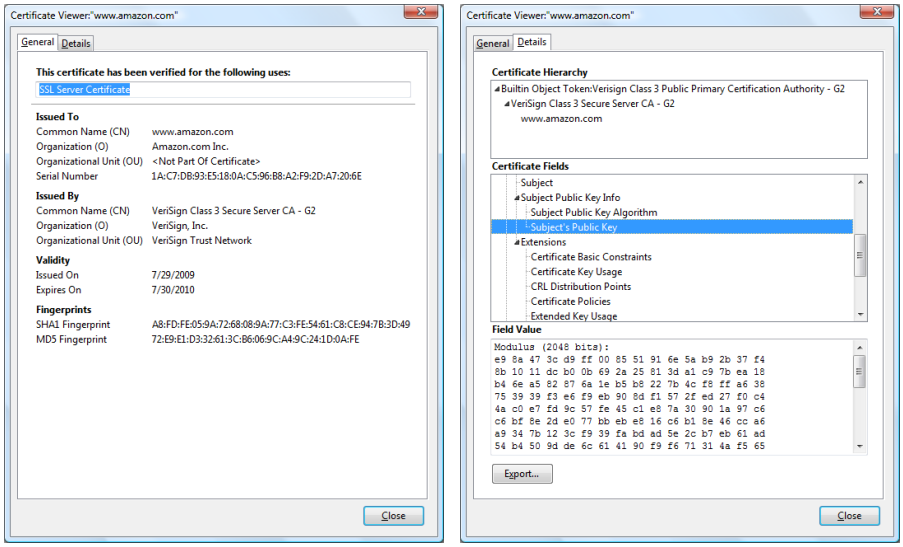
- Secure protocols use combination of techniques
- Big problem: public keys
  - System only works if public keys are correct

Secure Communication in Internet

- The Internet is big
  - Not everyone can know everyone
  - Not everyone can have shared keys with everyone
- Secure communication is necessary
  - Online banking, shopping, etc.
- Need to be able to verify identity of site
  - Even when never visited before
- Solution: trusted third party
  - Independent third party establishes mutual trust
  - Specifically: verifies correctness of parties' public keys
- Secure communication process
  - Use RSA algorithm to authenticate other party
  - Exchange symmetric session keys for communication
  - Use AES for bulk data exchange

Chain of Trust

- VeriSign certificate for www.amazon.com:



Chain of Trust

- SSL certificates from VeriSign:

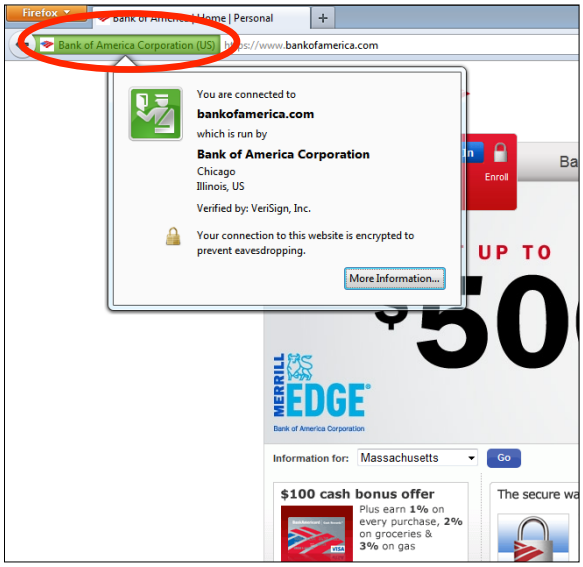
	Secure Site Pro with EV >>	Secure Site with EV >>	Secure Site Pro >>	Secure Site >>
Buy now	BUY	BUY	BUY	BUY
Renew	RENEW	RENEW	RENEW	RENEW
Trust level	★★★	★★★	★★☆	★★☆
Green address bar	✓	✓		
Extended validation	✓	✓		
VeriSign Secured® Seal	✓ VeriSign Secured	✓ VeriSign Secured	✓ VeriSign Secured	✓ VeriSign Secured
Full organization authentication	✓	✓	✓	✓
Security level	★★★	★★☆	★★★	★★☆
Encryption strength	128-bit minimum to 256-bit	40-bit minimum to 256-bit	128-bit minimum to 256-bit	40-bit minimum to 256-bit
NetSure® extended warranty	$250,000	$100,000	$250,000	$100,000
Express delivery			✓	
1-year validity	$1,499	$995	$995	$399
2-year validity	$2,695 *Save over $300*	$1,790 *Save $200*	$1,790 *Save $200*	$695 *Save over $100*
3-year validity			$2,480 *Save over $500*	$995 *Save over $200*

Chain of Trust

- Chain of trust can go multiple levels
  - Root certificates are final step
- Private keys need to protected well
- Security hardware:
  - Tamper-proof
  - On-board key generation
  - On-board cryptographic engine
  - E.g., IBM 4758 Cryptographic Coprocessor

Secure Web Browsing

- Watch for site identity shown in browser
  - Indicates secure connection (green)
  - Security certificate information available on clcik



Courses in ECE Curriculum

- ECE 597LL – Trustworthy Computing
- ECE 697AB – Security Engineering

Senior Design Project

- ECE Systems
  - Real world: many large systems
    - » See previous lectures
  - ECE curriculum: a few smaller systems
    - » Lab assignments in electronics lab, computer systems lab, etc.
    - » Larger system in Senior Design Project
- Today's lecture:
  - Senior Design Project (SDP)
    - » Overview
    - » 3 example projects

Senior Design Project

- Year-long team-based project course in senior year
- Goals of SDP
  - Realize an ECE system
  - Take system from idea to prototype
  - Work with an interdisciplinary team
- Other "side effects"
  - Learn to work in a team
  - Learn to give a professional presentation
  - Learn to deal with setbacks and design changes
  - Have something to talk about to recruiters
  - Have fun
- Main event of SDP: Senior Design Project Day
  - Friday 4/25/2014
  - 10 a.m. – 2:00 p.m.
  - Marcus / Gunness

Senior Design Project Day

- The big day…

SDP Projects

- Characteristics of SDP projects
  - New idea to solve a practical problem
    - » Potential for impact
  - Uses range of ECE technologies
    - » Embedded systems, software, networking, sensors, etc.
  - Right level of difficulty
    - » Not too easy, not too hard
- Web site with this year's projects:
  - http://www.ecs.umass.edu/ece/sdp/sdp14/teams.html

Courses in ECE Curriculum

- ECE 415 – Senior Design Project I
- ECE 416 – Senior Design Project II
- ECE 197DP/297DP/397DP – Design Project 1/2/3

Upcoming...

- Next Wednesday: Monday schedule
- Friday 4/25/14: Senior Design Project Day
  - SDP demos in Gunness
- Moodle quiz
- Wednesday in two weeks: RFID