CS 194-1 (CS 161)
Computer Security

Midterm 1
Review

Part 1

Threat Assessment

- Some questions:
  - What kind of threats might we face?
  - What kind of capabilities might we expect adversaries to have?
  - What are the limits on what the adversary might be able to do to us?

- Result is a *threat model*, a characterization of the threats the system must deal with
  - Think: *Who?* *What?* *Why?*

Security Basics

- Authentication: prove identity
  - Who are you?
- Authorization
  - Granting access
- Access control: enforcing authorization
  - Access Control Matrix
  - ACL
  - Capabilities

MAC and DAC

Mandatory Access Control (MAC)

- » We also use the abbreviation MAC for "message authentication code"
- » Policy determines access
- » Rules that the system enforces
- » Users can't break rules
- » RULES CAN BE FLEXIBLE

- Discretionary Access Control (DAC)
  - Users set their own rules
    - » (for their own files)

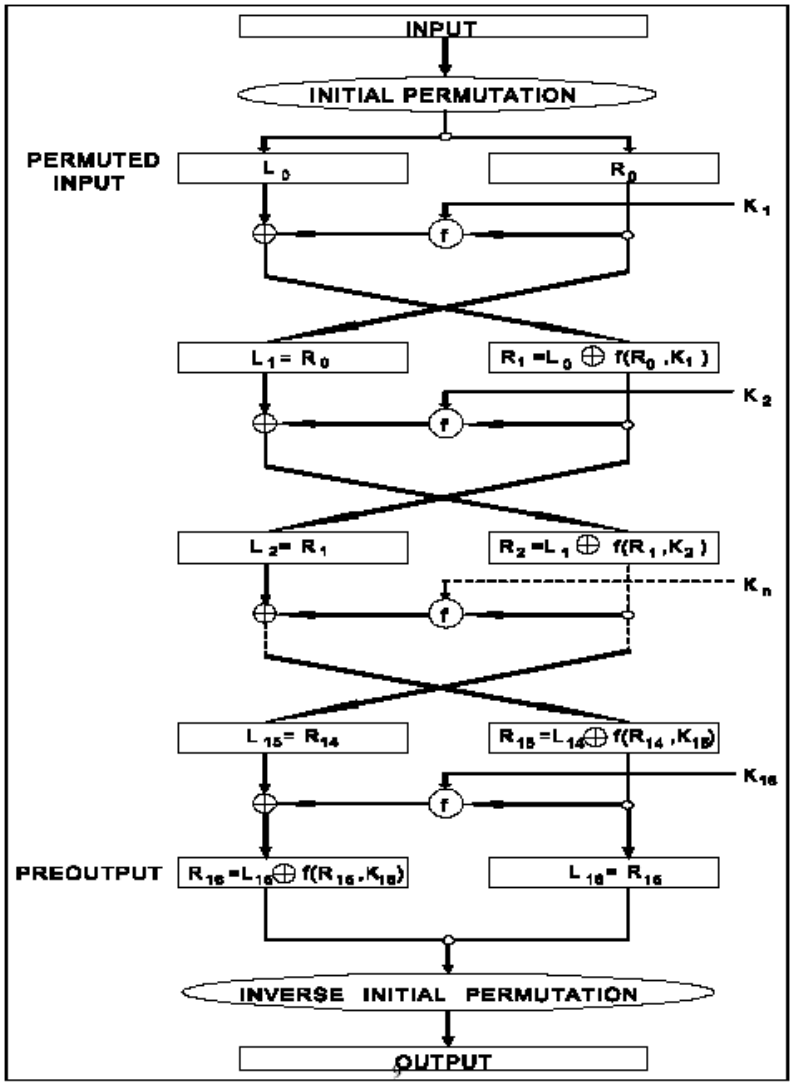
Symmetric crypto

- Definition
- Advantages
  - Fast
  - Reasonably well-understood
  - Standardized
  - Can be implemented in hardware easily
  - Exhaustive search attack hard (with large key size)

- Disadvantages
  - Key distribution
  - Single target
  - Still needs to be implemented in protocols

Symmetric Crypto: DES , AES

- AES (Rijndael)
- 128-256 bit key, 128 bit block cipher
- Attacks
  - Brute Force Exhaustive Search
  - Known Plaintext
  - Chosen Plaintext
    - » Differential cryptanalysis



Asymmetric: "public keys"

- Encryption key public, decryption key private
  - Easy way to send secret messages
  - Decryption only by intended recipient
  - Perfect for distributing symmetric keys

- Encryption key private, decryption key public
  - Only I can send messages, anyone can verify (and read)
  - A type of "digital signature"
  - We will develop this idea in detail

Asymmetric: pros and cons

- Advantages
  - Doesn't require advance set up
  - Strongest forms are as hard as factoring
  - Perfect for solving key distribution problem
  - Good for building protocols

- Disadvantages
  - Slow, slow, slow (& takes space too)
  - Secrecy & source authentication takes two encryptions
  - Need to find a way to prove "public keys" are honest
    - » Solution: public key hierarchy

RSA

- Rivest, Shamir, Adleman (1978 – published 1979)
- Idea:
  - Given e and d
  - Encryption: $c = E(m) = m^e \bmod pq$
  - Decryption: $D(c) = c^d \bmod pq$

- Issues:
  - Given e, how can we find d?
    - » Answer: use EGCD (extended greatest common divisor)
      - Euclidean algorithm

Signatures

- Signing vs. Encrypting
- Encryption is a TOOL
  - Can help in signing
  - Does not trivially solve the signature problem!

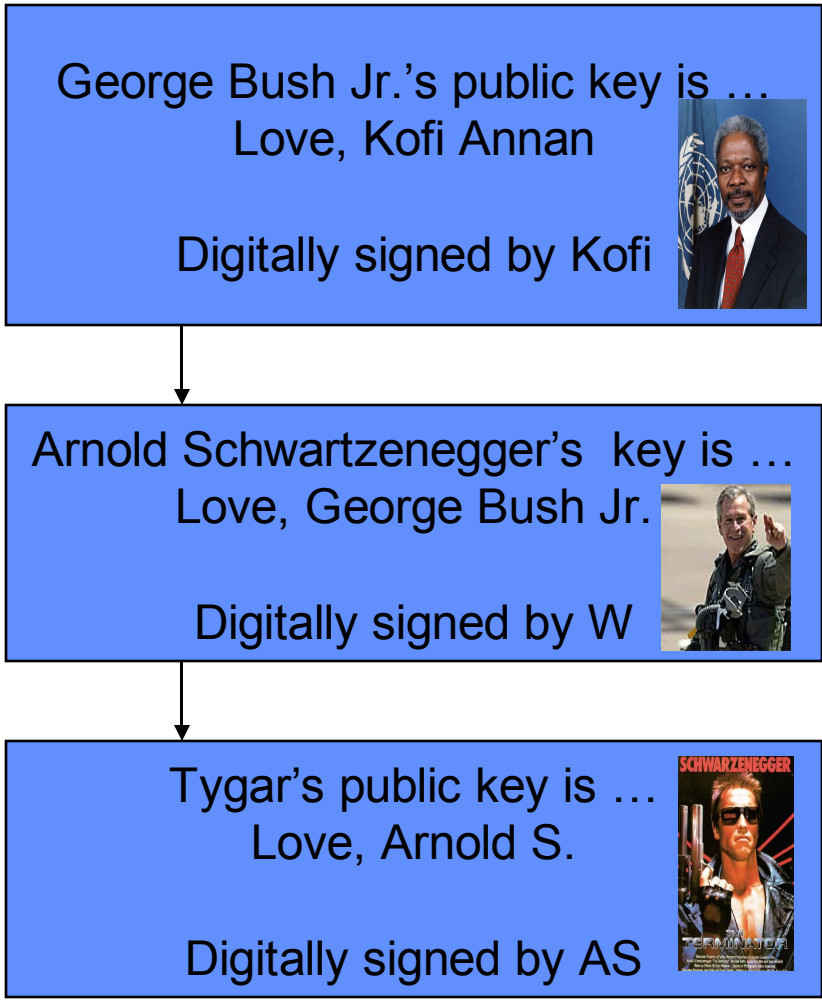
- Asymmetric Signing
  - Pretty Secure
  - Slow!

- Symmetric Encryption As Signature?
  - Faster… but We need non-repudiation

- Message Authentication Code
  - Sign a hash!
    - » FAST, also ensures integrity

PKI: Public Key Infrastructure

- Problem: Whose public key is it?
- Solution: Have a trustworthy person sign it to vouch.
- Problem: Very few people are trusted by the WHOLE WORLD
  - Too much work on them!
- Solution: Delegation
  - Kofi delegates to presidents/kings.
  - President delegates to governors.



Revocation

- What?
  - Declare a public key to be invalid
- Why?
  - Private key stolen
  - Failed PKI
- How?
  - Explicit Revocation (lists)
    - » As Needed
  - Automatic Expiration
    - » Expiration date