CN414
Computer Network Security

Week 3:- Encryption and Decryption

By

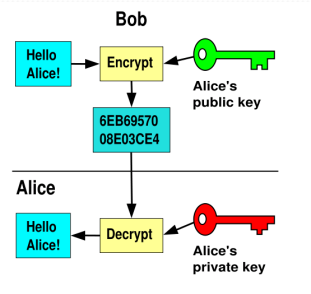
Dr. Piya Techateerawat

Encryption & Decryption

- **Encryption & Decryption Concept**
- Symmetric Key Encryption
- Asymmetric Key Encryption
- Encryption Protocols

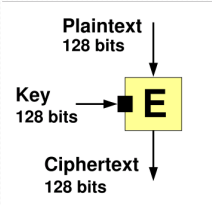
Encryption & Decryption Concept

- Encryption is the practice to keep the information available for only related parties.



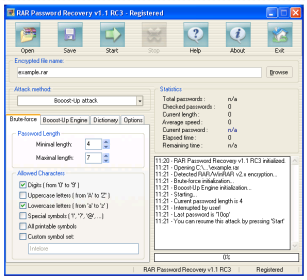
Encryption & Decryption Concept

- **Stream Ciphers:-** Input plaintext can be encoded to the output a stream of cipher text
- **Block Ciphers:-** To encrypt & decrypt information in fixed size blocks



Encryption & Decryption Concept

- **Cryptanalysis:-** To break the cipher or code by using high skill of mathematical analysis.
- **Brute Force:-** To attempt to break the cipher by trying every possible combination of keys.

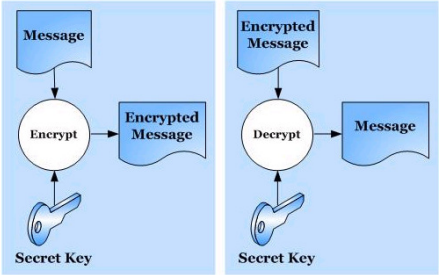


Encryption & Decryption

- Encryption & Decryption Concept
- **Symmetric Key Encryption**
- Asymmetric Key Encryption
- Encryption Protocols

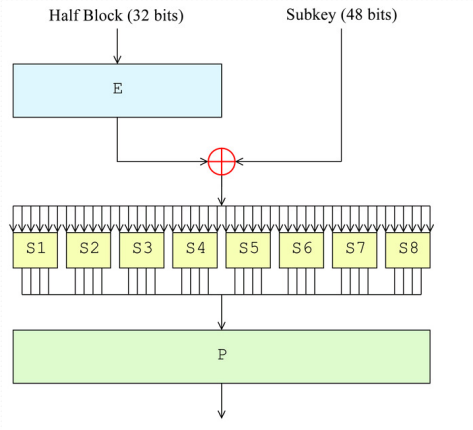
Symmetric Key Encryption

- The same single key or secret key is used on both encryption and decryption.
- Strength:- Simple, Fast, low computation
- Weakness:- Requires secret sharing, Complex admin



Symmetric Key Encryption

- DES:- Data Encryption Standard

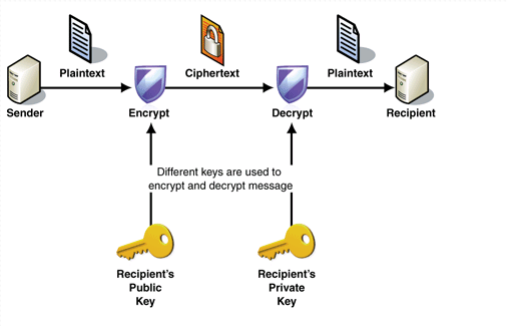


Encryption & Decryption

- Encryption & Decryption Concept
- Symmetric Key Encryption
- **Asymmetric Key Encryption**
- Encryption Protocols

Asymmetric Key Encryption

- Using to key in the process, one key is for encryption where another key is for decryption.



Asymmetric Key Encryption

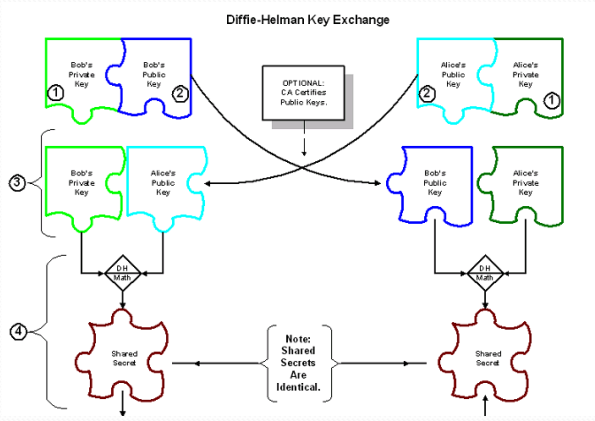
- Public Key

  Mainly use in

  1. **Diffie-Hellman**:- Combination of Public key to generate symmetric key
  2. **RSA**:- Using large prime number to generate keys.
  3. **Digital Signature Algorithm**:- To verify the correctness of message.

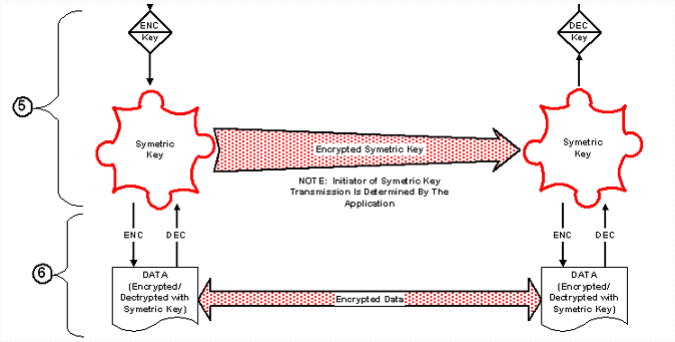
Asymmetric Key Encryption

- Diffie-Hellman



Asymmetric Key Encryption

- Diffie-Hellman



Asymmetric Key Encryption

- RSA

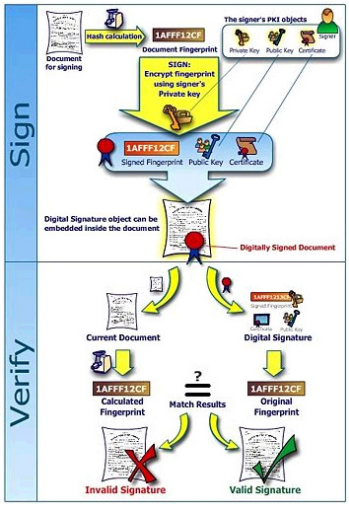
RSA Algorithm: Example

- Select two large primes: p, q, p ? q
  p = 17, q = 11
- n = p×q = 17×11 = 187
- Calculate Φ = (p-1)(q-1) = 16x10 = 160
- Select e, such that lcd(Φ, e) = 1; 0 < e < Φ
  say, e = 7
- Calculate d such that de mod Φ = 1
  - 160k+1 = 161, 321, 481, 641
  - Check which of these is divisible by 7
  - 161 is divisible by 7 giving d = 161/7 = 23
- Key 1 = {7, 187}, Key 2 = {23, 187}

Washington University in St. Louis CSE574s ©2005 Raj Jain

Asymmetric Key Encryption

- Digital Signature



Case Study

Ian Goldberg
Assistant Professor
David R. Cheriton School of Computer Science
University of Waterloo
200 University Ave W
Waterloo, Ontario, Canada
N2L 3G1

Office: DC 3518
Phone: 519-888-4567 x36168

Case Study

- A graduate student at the University of California at Berkeley used a network of about 250 workstations to crack a 40-bit algorithm in less than four hours yesterday, a university professor told CNET today. Responding to an international contest announced by encryption software company RSA Security Dynamics, grad student Ian Goldberg set the UC Berkeley Network of Workstations to the task of cracking the code yesterday using cryptanalysis software, key-testing software that he "tweaked" to run even faster than usual. The software was able to test about 100 billion key combinations an hour, said Eric Brewer, the Berkeley computer science professor who oversees Goldberg's work with the Internet Security, Applications, Authentication and Cryptography research group.
- For his efforts, Goldberg won the $1,000 prize for the 40-bit level, the weakest encryption that RSA offers. His ease in completing the hack adds fuel to the argument that 40-bit crypto, where scrambling codes are composed of a string of 40 digits, is too weak for commercial use.

Case Study

- "If we can break a random 40-bit key in three-plus hours, it means Internet commerce based on 40-bit keys is unacceptable," Brewer said.
- Longer bit lengths make cracking exponentially more difficult, however. A 56-bit algorithm would take about 22 years to crack under similar circumstances, Brewer said.
- There is no limit on the strength of encryption used domestically, but newly revised U.S. export regulations have set a provisional limit of 56-bit algorithms as long as the exporter agrees to support a system of key storage that allows the government access to encrypted data.
- The ISAAC group made news last fall when it cracked the encryption layer of Netscape Communications' Navigator browser. In that case, Netscape programmers had failed to select completely random bits for their encryption algorithms.
- Brewer and his staff were able to detect patterns in the string of digits and crack the code fairly easily. Netscape immediately fixed the problem and re-released the browser.

Q & A