1 Administrivia

Announcements

Assignment

From Last Time

Phil Zimmermann video.

Outline

1. DES.
2. AES.
3. Public key principles.
4. Uses.

Coming Up

Discussion of individual Perl/CGI assignment and project.
2  

DES

1. IBM-designed and NSA-analyzed.
   (a) 64-bit block cipher. Symmetric.
   (b) Uses simple arithmetic and logical operations.
   (c) Slow — hardware implementations were available. (But faster than asymmetric.)
   (d) Sixteen rounds of substitution and transposition.

2. Controversy:
   (a) 128 bit keys to 64 to 56 (parity bits).
   (b) Design of S-boxes.

3. Differential cryptanalysis shows that DES is “optimal.”
   This technique was known to IBM and the NSA much earlier.

2.1 Marginally Increased Strength: Double DES

1. Product cipher — apply DES twice, with two keys.
   \[ C = E(k_2, E(k_1, P)) \]

2. With two keys, should have strength of \(2^{2\times56}\), right?

3. Wrong — strength is \(2^{1+56}\), using “Meet in the Middle” attack.
   Requires two plaintext, ciphertext pairs.

2.2 Reasonably Increased Strength: Triple DES

1. Apply DES three times, with two keys.
\[ C = E(k_1, D(k_2, E(k_1, P))) \]

Why a decrypt stage? Consider the case \( k_2 = k_1 \) — single DES.

2. Strength is apparently \( 2^{112} \).

Meet in the middle attack not effective.

## 3 AES

1. Replaces DES as a US standard.

2. Winner of a “contest.” Designed by two Dutch cryptographers (Rijndael).
   Vetted by NSA.

3. 128-bit block cipher. Symmetric.

4. Uses simple arithmetic and logical operations.

5. Fast and easy to implement.

   Key lengths of 192 and 256 are approved for US Top Secret level data.

7. Number of rounds is a function of key length: 9, 11, 13.
   Decreasing the number of rounds weakens AES. To date, best known attacks are with 7, 8, 9 rounds, respectively. Too close for comfort?

   What do we mean by breaking encryption?

## 4 Public Key Encryption

General principles:

1. Asymmetric.
2. \( P = D(k_{\text{PRIV}}, E(k_{\text{PUB}}, P)). \)
   Also: \( P = E(k_{\text{PUB}}, D(k_{\text{PRIV}}, P)). \)

3. 10,000 times slower than private key.

4. RSA based on finding the two prime factors of a large number.

5 \textbf{Uses}

Elements:

1. Symmetric cipher for private data transfer.
   Key distribution?

2. Asymmetric for initial privacy, authentication.
   E for privacy, D for authentication.
   \textit{How} can “someone” securely send you a document?
   \textit{How} do I convince you of my identity?
   \textit{How} do I securely send you a document, convincing you it’s from me?

3. Hash (MD5) for digestification and digital signature.

Requirements for secure information transfer between two parties. Information should be:

1. Unforgeable.

2. Authentic.

3. Unalterable.

How do we use the former elements so as to provide these features?

Digital certificate:

1. An originator’s identity and public key.
2. CA certifies.
3. Digest and sign by CA.
4. Return to originator, who verifies.

What is the goal of SSL? How does it work?