Class Notes Oct 31 2017

Derek Stachowiak

November 30, 2017

Finishing SAES example
End round 1: 0010 1110 0100 1011
Substitute(Feed into S-Box): 1010 1111 1101 0011
Put results from previous step into a matrix by filling down the rows $\begin{bmatrix}1010 & 1101\\1111 & 0011\end{bmatrix}$
Shift columns $\begin{bmatrix}1010 & 1101\\0011 & 1111\end{bmatrix}$
Read down columns: 1010 0011 1101 1111
xor with round key: 1000 0111 1010 1111
C= 0010 0100 0111 0000

AES:
10 Rounds
Skip mix columns in last round
128 bits of plain text
key is 128, 196 or 256 bits in length
Differential cryptoanalysis is faster than brute force for 7 rounds. For this reason 10 rounds was chosen to be secure against future attacks.
almost all secure internet fraffic uses AES

The problem is you need the key to encrypt or decrypt. AES and DES are examples of symetric key algorithms, i.e. both Alice and Bob need the key and if anyone finds the key then the system is compromised.

Big Innovation
Pubic key cryptography
Allows messages to be sent securely between two people who have no shared secret key

Public key cryptography
Relies on trap door problem
Trap door problem: math problem that is easy to do one way but very difficult the other way

Mathematician Rivest,Adelman and Shamir came up with RSA
Trap door problem: Factoring
Take two primes p,q
Easy to multiply n = p * q
Very hard to find p and q given n
Five steps to RSA
Alice will pick two prime numbers p,q(120ish digits in length)
n = p * q
She picks encryption exponent e (65537 is common)
She publishes (n,e)
Alice computes φ(n) = (p-1)(q-1) (this is secret!)
Compute $d = e^{-1} (\text{mod } \varphi(n))$ using Euclids algorithm
d is the decryption key (secret)