CS641

Modern Cryptology

Lecture 9

History

- By the end of 1990s, key size of DES became amenable to brute-force attack:
  - In 1999, a distributed brute-force search recovered DES key within one day
- In 1997, National Institute of Standards and Technology (US), announced a worldwide call for a new standard algorithm.
- Fifteen proposals were submitted and eventually Rijndael, developed by two Belgian cryptographers, Vincent Rijmen and Joan Deamen, was adopted as Advanced Encryption Standard (AES) in 2001.

AES: Details

- Blocksize: 128 bits
- Keysize: 128, 192, or 256 bits
- Number of rounds: 10, 12, or 14
- Each round has four operations in a sequence: ByteSub, ShiftRow, MixColumn, AddRoundKey.
- Round keys are generated from the key using a fixed schedule.

Viewing a Block

- A block is 128 bits, or 16 bytes long.
- It is viewed as an element of $F_{256}^{4\times 4}$.
- In other words, a block is treated as a 4×4 matrix with elements from F_{256}:

$$B = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

AES Operations: ByteSub

ByteSub

$$b_{ij} = \begin{cases} \frac{1}{a_{ij}} & \text{if } a_{ij} \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

$$c_{ij} = T \cdot b_{ij} + c$$

T is a fixed 8×8 invertible matrix over F_2 and c is a fixed column vector over F_2.

- In F_{256}^*, $1/a_{ij} = a_{ij}^{254}$ since $a_{ij}^{255} = 1$.
- The only non-linear operation.
- Easily seen to be invertible.

AES Operations: ShiftRow

ShiftRow

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \Rightarrow \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{11} & a_{12} & a_{13} & a_{10} \\ a_{22} & a_{23} & a_{20} & a_{21} \\ a_{33} & a_{30} & a_{31} & a_{32} \end{bmatrix}.$$

- A left-rotation of i columns is applied on ith row
- Each column in new matrix consists of one element from every column of old matrix

AES Operations: MixColumn

MixColumn

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

- A fix matrix is multiplied to block matrix.
- Viewing each column as a degree three polynomial in $F_{256}[x]$, the operation is same as multiplying column polynomial by fixed polynomial $3x^3 + x^2 + x + 2$ modulo $x^4 + 1$.

AES Operations: AddRoundKey

AddRoundKey

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \Rightarrow \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} + \begin{bmatrix} k_{00} & k_{01} & k_{02} & k_{03} \\ k_{10} & k_{11} & k_{12} & k_{13} \\ k_{20} & k_{21} & k_{22} & k_{23} \\ k_{30} & k_{31} & k_{32} & k_{33} \end{bmatrix}.$$

- Round key matrix is added to block matrix.
- Addition is bitwise XOR in F_{256}.
- Each round key matrix is derived from key using a fixed algorithm.

AES: Rounds

- Number of rounds are 10, 12, or 14 depending on key size chosen.
- There is one additional AddRoundKey operation performed before the first round.
- Last round does not have MixColumn operation.
- In our analysis, we will focus on 10 round AES with 128 bit key, the most commonly used variant.

Observations on AES

- MixColumn is only operation that "mixes" elements of a block.
- Together with ShiftRow, in two rounds all elements get mixed up.
- Each operation is easily seen to be invertible, making decryption possible.
- ByteSub is only non-linear operation – its linear part chosen so that at least one operation is not within F_{256}.

AES Decryption

- The rounds and ordering of round operations get reversed.
- AddRoundKey remains the same, except that the use of round keys is reversed.
- ShiftRow and ByteSub can be exchanged.
- AddRoundKey and MixColumn can be exchanged:

$$M \cdot (B + K) = M \cdot B + M \cdot K.$$

- Since MixColumn is not used in last round, MixColumn and AddRoundKey of second last encryption round can be exchanged and viewed as operations in first decryption round.
- This allows sequence of operations in encryption and decryption to be identical.

AES: One Round

- The sequence of operations are:
  $$\textit{AddRoundKey} \rightarrow \textit{ByteSub} \rightarrow \textit{ShiftRow} \rightarrow \textit{AddRoundKey}$$
- No MixColumn as this is the last round also.
- There is no mixing — so encryption is byte-by-byte.
- Thus it can be broken with a 256 byte chosen-plaintext attack.

AES: Two Rounds

- The sequence of operations are:
  $AddRoundKey \rightarrow ByteSub \rightarrow ShiftRow \rightarrow MixColumn \rightarrow AddRoundKey \rightarrow ByteSub \rightarrow ShiftRow \rightarrow AddRoundKey$
- There is some mixing now, but still it is only on four byte groups.
- Therefore, it can be broken with a $2^{32} \approx 4GB$ chosen-plaintext attack.

AES: Three Rounds

- With MixColumn in two rounds, entire block is mixed up, so a simple brute-force attack is not feasible.
- With keys being XORed, we can use differential cryptanalysis to try to remove its effect, as in DES.
- Let x and $x + d_0$ be two values of a plaintext byte with fixed difference d_0.
- The difference remains the same after AddRoundKey operation.
- It becomes $\frac{1}{x} + \frac{1}{x+d_0} = \frac{d_0}{x(x+d_0)}$ after non-linear part of ByteSub.
- The probability, over choices of x, that the difference now equals to a specific value is at most $\frac{1}{128}$ provided $d_0 \neq 0$.

AES: Three Rounds

- Fixing difference of all other bytes in a block to zero will maximize the probability of difference being a fixed value after the ByteSub.
- After MixColumn, this difference will propagate to four bytes.
- Hence, after first round, we get four bytes with a non-zero difference.

AES: Three Rounds

- Difference after ByteSub of second round will be a fixed value with probability less than $\frac{1}{2^{28}}$ since four bytes have non-zero difference.
- MixColumn of second round will spread non-zero difference to all sixteen bytes.
- This will make probability of knowing difference after third round ByteSub extremely small.
- Other simple variations of differential cryptanalysis also fail on three round AES.
- Attempting a linear cryptanalysis approach results in similar failure.

AES: Three Rounds

- AES was designed to be resistant against differential and linear cryptanalysis.
- A modified form of differential cryptanalysis, called square attack, does break three round AES.
- In this attack, we consider a set of 256 plaintext blocks being encrypted simultaneously and trace patterns of byte values.