CS641

Modern Cryptology

Lecture 7

DES: Four Rounds

- Let $E(R_3) = \alpha_1\alpha_2 \cdots \alpha_8$ and $E(R_3') = \alpha_1'\alpha_2' \cdots \alpha_8'$ with $|\alpha_i| = 6 = |\alpha_i'|$.
  - R_3 and R_3' are right-halves of output of third round on the plaintexts L_0R_0 and $L_0'R_0' = L_0'R_0$.
- Let $\beta_i = \alpha_i \oplus k_{4,i}$ and $\beta_i' = \alpha_i' \oplus k_{4,i}$, $|\beta_i| = 6 = |\beta_i'|$.
  - $k_4 = k_{4,1}k_{4,2} \cdots k_{4,8}$.
- Let $\gamma_i = S_i(\beta_i)$ and $\gamma_i' = S_i(\beta_i')$, $|\gamma_i| = 4 = |\gamma_i'|$.
- We know α_i, α_i' and $\beta_i \oplus \beta_i' = \alpha_i \oplus \alpha_i'$.
- We also know a value γ such that $\gamma_i \oplus \gamma_i' = \gamma$ with probability $\frac{14}{64}$.

DES: Four Rounds

- Define

$$X_i = \{(\beta, \beta') \mid \beta \oplus \beta' = \beta_i \oplus \beta'_i \text{ and } S_i(\beta) \oplus S_i(\beta') = \gamma\}.$$

- Pair $(\beta_i, \beta'_i) \in X_i$ whenever our guess for $\gamma_i \oplus \gamma'_i = \gamma$ is correct, which happens with probability $\frac{14}{64}$.
- Define

$$K_i = \{k \mid \alpha_i \oplus k = \beta \text{ and } (\beta, \beta') \in X_i \text{ for some } \beta'\}.$$

- Since $(\beta_i, \beta'_i) \in X_i$ with probability $\geq \frac{14}{64}$, we have $k_{4,i} \in K_i$ with probability $\geq \frac{14}{64}$.

DES: Four Rounds

- We have $|K_i| = |X_i|$ since α_i and $\beta \oplus \beta'$ is fixed for $(\beta, \beta') \in X_i$.
- Therefore, $|K_i| \leq 16$ as per properties of S-boxes.
- We cannot use the method for three rounds here:
  - If we compute another K_i' and take its intersection with K_i, $k_{4,i}$ may get dropped out since it is not guaranteed to be present in both.

DES: Four Rounds

- Instead, we do as follows.
- Let $K_{i,1}$, $K_{i,2}$, ..., $K_{i,\ell}$ be set of possible subkeys, each containing $k_{4,i}$ with probability $\geq \frac{14}{64}$.
  - The probability is over random choices of plaintext pairs satisfying the given XOR condition.
- Then the expected number of sets containing $k_{4,i}$ would be $\geq \frac{14}{64}\ell$.
- On the other hand, consider a value $a \neq k_{4,i}$.
  - We assume that $\Pr[a \in K_{i,s}] = \frac{|K_{i,s}|}{64}$.
  - Then, expected number of sets containing a would be $\frac{1}{64}\sum_{s=1}^{\ell} |K_{i,s}| \leq \frac{16}{64}\ell$.
- If sets $K_{i,s}$ have sizes close to 16, then an incorrect value a seems to occur equally frequently as $k_{4,i}$!

DES: Four Rounds

- On careful analysis, we get:
  - If $\gamma \neq \gamma_i \oplus \gamma_i'$ then $k_{4,i}$ becomes wrong value.
  - Hence, $\Pr[k_{4,i} \in K_{i,s} \mid \gamma \neq \gamma_i \oplus \gamma_i'] = \frac{|K_{i,s}|}{64}$.
  - Therefore, expected number of sets containing $k_{4,i}$ would be

$$\geq \frac{14}{64}\ell + \sum_{\substack{1 \leq s \leq \ell \\ \gamma \neq \gamma_i \oplus \gamma_i' \text{for } s}} \frac{|K_{i,s}|}{64}.$$

- In comparison, expected number of sets containing $a \neq k_{4,i}$ would be

$$= \sum_{\substack{1 \leq s \leq \ell \\ \gamma = \gamma_i \oplus \gamma_i' \text{for } s}} \frac{|K_{i,s}|}{64} + \sum_{\substack{1 \leq s \leq \ell \\ \gamma \neq \gamma_i \oplus \gamma_i' \text{for } s}} \frac{|K_{i,s}|}{64}.$$

DES: Four Rounds

- Gap between the two numbers is minimum when all $K_{i,s}$ have maximum possible size, i.e., 16.
- Then the number for $k_{4,i}$ is:

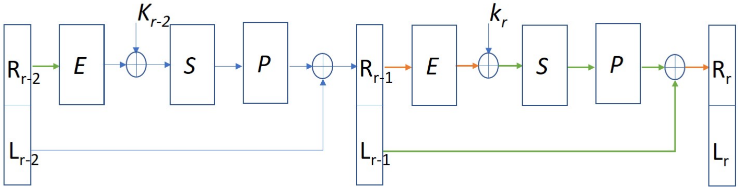
$$\geq \frac{14}{64}\ell + \frac{12.5}{64}\ell = \frac{26.5}{64}\ell.$$

- And the number of $a \neq k_{4,i}$ is:

$$= \frac{16}{64}\ell.$$

- Choosing $\ell \geq 20$ would give sufficient gap between the two expected values.
- Then $k_{4,i}$ can be identified as the most frequently occurring value in the sets $K_{i,1}$, $K_{i,2}$, ..., $K_{i,\ell}$.

DES: r Rounds



- For r round DES, we extend the approach used for four rounds:
  - Predict the XOR of output of round $r-2$ with as high probability as possible
  - This allows for prediction of output XOR for S-boxes of last round.
  - Coupled with knowledge of both outputs of last round E, we can extract last round key as in four round DES.
- In order to find XOR of output of round $r-2$, we define notion of characteristic.

Characteristic

An *s-round characteristic* is a sequence $(x_0, y_0, p_1, x_1, y_1, p_2, x_2, y_2, \ldots, p_s, x_s, y_s)$ where

- $|x_i| = 32 = |y_i|$.
- When XOR of the output of round i equals $x_i y_i$, then the XOR of the output of round $i+1$ equals $x_{i+1} y_{i+1}$ with probability p_{i+1}.

- $(6000\bar{0}, \bar{0}\bar{0}, 1, \bar{0}\bar{0}, 6000\bar{0}, \frac{14}{64}, 6000\bar{0}, 00828000)$ is a 2-round characteristic as seen above.
  - $\bar{0}$ stands for 16-bit string 0000.

Characteristic

Probability of a Characteristic

The probability of an s-round characteristic $(x_0, y_0, p_1, x_1, y_1, p_2, x_2, y_2, \ldots, p_s, x_s, y_s)$ equals $\prod_{i=1}^{s} p_i$.

- Probability of a characteristic denotes the probability, over the choice of plaintext block pairs with XOR equal to $x_0 y_0$, that XOR of the outputs of ith round, $1 \leq i \leq s$, equals $x_i y_i$.
- Probability of 2-round characteristic $(6000\bar{0}, \bar{0}\bar{0}, 1, \bar{0}\bar{0}, 6000\bar{0}, \frac{14}{64}, 6000\bar{0}, 00828000)$ equals $\frac{14}{64}$.

Breaking r-round DES

- To break r-round DES, we need an $r-2$ round characteristic:
  - We recover k_r using this characteristic.
  - If the probability of characteristic is p, and we use ℓ paintext block pairs, $k_{r,i}$ will be present in about $p\ell + (1-p)\frac{\ell}{4}$ X_i's.
  - Any other $a \neq k_{r,i}$ will be present in about $\frac{\ell}{4}$ pairs.
  - So $k_{r,i}$ is present is roughly $\frac{3}{4}p\ell$ additional pairs.
  - We need $\ell \approx \frac{20}{p}$ in order to ensure that $k_{r,i}$ is most frequently occurring value.
- This technique is called differential cryptanalysis.
  - Proposed by Biham and Shamir in 1990.

Example Characteristics

- 3-round characteristic:

$$(00828000, 6000\bar{0}, \tfrac{14}{64}, 6000\bar{0}, \bar{0}\bar{0}, 1, \bar{0}\bar{0}, 6000\bar{0}, \tfrac{14}{64}, 6000\bar{0}, 00828000).$$

- Another 3-round characteristic:

$$(4008\bar{0}, 0400\bar{0}, \tfrac{1}{4}, 0400\bar{0}, \bar{0}\bar{0}, 1, \bar{0}\bar{0}, 0400\bar{0}, \tfrac{1}{4}, 0400\bar{0}, 4008\bar{0}).$$

- A 5-round characteristic:

$$(405C\bar{0}, 0400\bar{0}, \tfrac{1}{4}, 0400\bar{0}, 0054\bar{0}, \tfrac{5}{128}, 0054\bar{0}, \bar{0}\bar{0}, 1, \bar{0}\bar{0}, 0054\bar{0}, \tfrac{5}{128}, 0054\bar{0}, 0400\bar{0}, \tfrac{1}{4}, 0400\bar{0}, 405C\bar{0})$$

Iterative Characteristics

- 2-round characteristic:

$$(\bar{0}\bar{0}, 1960\bar{0}, \frac{1}{234}, 1960\bar{0}, \bar{0}\bar{0}, 1, \bar{0}\bar{0}, 1960\bar{0}).$$

- This can be concatenated r times to create a $2r$-round characteristic.
- The probability of $2r$-round characteristic will be $\frac{1}{(234)^r}$.
- Can be used against 16-round DES:
  - Probability of characteristic will be $\frac{1}{(234)^7} \approx \frac{1}{2^{55}}$.
  - The number of plaintext pairs required would be $\approx 2^{59}$, worse than brute-force.

15-round DES

- Invert the 2 round characteristic to:

$$(19600\bar{0}, \bar{0}\bar{0}, 1, \bar{0}\bar{0}, 19600\bar{0}, \tfrac{1}{234}, 19600\bar{0}, \bar{0}\bar{0}).$$

- Concatenating for 13-rounds gives a characteristic with probability $\frac{1}{(234)^6} \approx \frac{1}{2^{47}}$.
- The number of plaintext pairs required to break it are $\approx 2^{52}$, which is less than brute-force.
- Therefore, 16 is the minimum number of rounds that makes DES fully resistant against differential cryptanalysis.

Linear Cryptanalysis

- Proposed by Matsui in 1994.
- Exploits partial linearity present in S-boxes.
- Breaks 16-round DES with a known plaintext attack using around 2^{47} plaintext blocks.
- Only known method of breaking 16-round DES faster than brute-force.

Linearity in S5

- Let $b_0 b_1 \cdots b_5$ be input bits to S-box S5, and $c_0 c_1 c_2 c_3$ be output bits.
- Then,

$$b_1 \oplus c_0 \oplus c_1 \oplus c_2 \oplus c_3 = 0$$

  with probability $\frac{12}{64}$.
- For round i, $L_{i-1}R_{i-1}$ is input and $L_i R_i$ is output.
- Let $R_i[j]$ denote the jth bit of R_i, $0 \leq j \leq 15$, and $R_i[j_1, j_2, \ldots, j_s] = \oplus_{t=1}^{s} R_i[j_t]$.
- The above equation can be written for round i as:

$$R_{i-1}[15] \oplus K_i[22] \oplus L_{i-1}[7, 18, 24, 29] \oplus R_i[7, 18, 24, 29] = 0$$

  with probability $\frac{12}{64}$.

DES: Three Rounds

- Using previous equation for round 1, we get that with probability $\frac{12}{64}$:

$$\begin{aligned} R_0[15] \oplus K_1[22] \oplus L_0[7,18,24,29] &= R_1[7,18,24,29] \\ &= L_2[7,18,24,29] \\ &= R_3[7,18,24,29] \oplus f(R_2,K_3)[7,18,24,29] \end{aligned}$$

  where $f(R,K)$ is the non-linear function of DES.
- Therefore,

$$R_0[15] \oplus L_0[7,18,24,29] \oplus R_3[7,18,24,29] \oplus f(R_2,K_3)[7,18,24,29] = K_1[22]$$

  with probability $\frac{12}{64}$.

DES: Three Rounds

- Since we know R_0, L_0, R_3, and $R_2 = L_3$, we can do following:
  - Guess six bits of K_3 that go into S5.
  - For ℓ choices of plaintext block, and using the guess of K_3, compute how many times is LHS zero.
- If guess for K_3 is wrong, the equation will be satisfied roughly half the time.
- If guess is correct, either LHS would be zero about $\frac{12}{64}\ell$ times or LHS would be 1 about $\frac{12}{64}\ell$ times.
- This gives us six bits of K_3 and one bit of K_1.
- Doing the same for third round gives one bit of K_3 and six bits of K_1, resulting in a total of 14 bits of key overall.

DES: Sixteen Rounds

- This can be extended to an equation for 16 round DES:

$$
\begin{aligned}
& L_0[7, 18, 24] \oplus R_0[12, 16] \oplus L_{16}[15] \oplus R_{16}[7, 18, 24, 29] \oplus f(R_{15}, K_{16})[15] \\
= \quad & K_1[19, 23] \oplus K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \oplus \\
& K_8[44] \oplus K_9[22] \oplus K_{11}[22] \oplus K_{12}[44] \oplus K_{13}[22] \oplus K_{15}[22]
\end{aligned}
$$

- The equation holds with probability $\approx \frac{1.2}{2^{22}}$.
- Using $\approx 2^{47}$ plaintext blocks, 14 bits of key can be recovered.
- Remaining 42 bits can be found by brute-force, resulting in overall complexity of $\approx 2^{47}$.