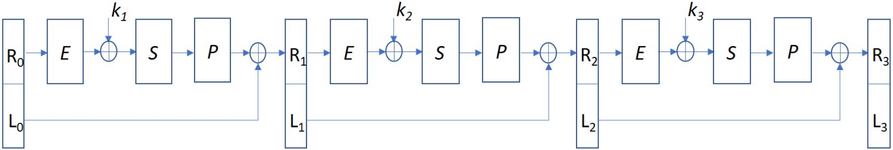
CS641

Modern Cryptology

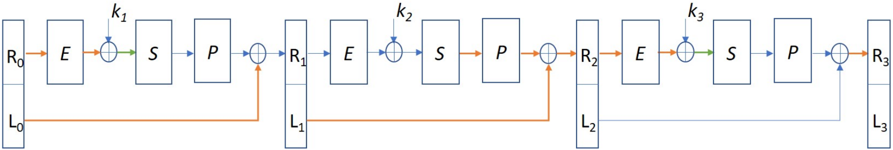
Lecture 6

DES: Three Rounds



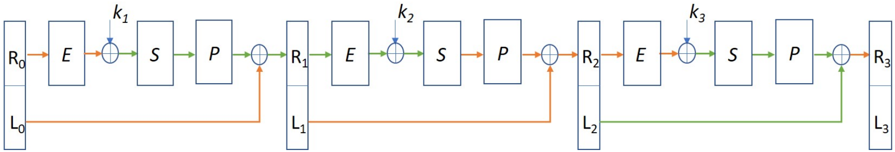
- Let $L_0 R_0$ be a plaintext block and $L_0' R_0'$ be another.
- How does their XOR travel through encryption stages?
- Let us identify locations where we know the XOR values.

DES: Three Rounds



- XOR values in all lines marked green are known.
- Only two additional values become known.
- Choose $R_0 = R_0'$.

DES: Three Rounds



- XOR values in all remaining lines are known now.
- Particularly, in third round, actual values of output from *E* and XOR values of output from S-boxes is known.
- This gives a way to break the encryption.

DES: Three Rounds

- Let $E(R_2) = \alpha_1\alpha_2\cdots\alpha_8$ and $E(R_2') = \alpha_1'\alpha_2'\cdots\alpha_8'$ with $|\alpha_i| = 6 = |\alpha_i'|$.
  - R_2 and R_2' are right-halves of output of second round on the plaintexts L_0R_0 and $L_0'R_0' = L_0'R_0$.
- Let $\beta_i = \alpha_i \oplus k_{3,i}$ and $\beta_i' = \alpha_i' \oplus k_{3,i}$, $|\beta_i| = 6 = |\beta_i'|$.
  - $k_3 = k_{3,1}k_{3,2}\cdots k_{3,8}$.
- 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', $\beta_i \oplus \beta_i' = \alpha_i \oplus \alpha_i'$, and $\gamma_i \oplus \gamma_i'$.

DES: Three Rounds

- Define

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

- Pair $(\beta_i, \beta'_i) \in X_i$.
- Define

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

- Since $(\beta_i, \beta'_i) \in X_i$, we have $k_{3,i} \in K_i$.

DES: Three Rounds

- We have $|K_i| = |X_i|$ since α_i and $\beta \oplus \beta'$ is fixed for $(\beta, \beta') \in X_i$.
- If $|X_i| < 64$ then we have eliminated some possibilities of $k_{3,i}$.
- As done earlier, we can then repeat for multiple pairs of plaintexts to reduce the possibilities further until $k_{3,i}$ is uniquely identified.
- What if $|X_i| = 64$?
  - Then for every β, $S_i(\beta) \oplus S_i(\beta \oplus \beta_i \oplus \beta_i') = S_i(\beta \oplus \beta') \oplus S_i(0)$, or equivalently

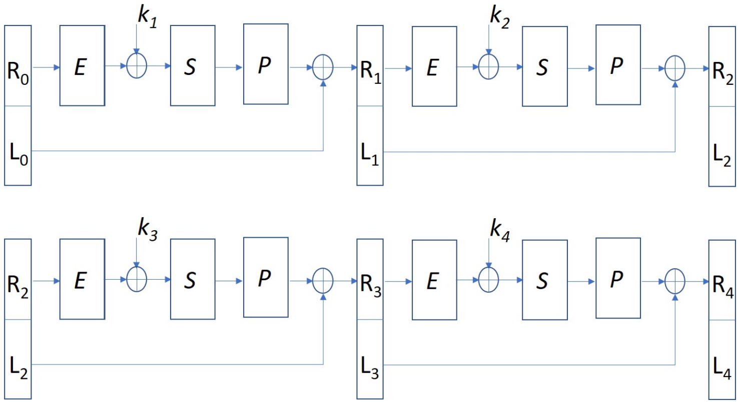
$$S_i(\beta \oplus \beta_i \oplus \beta_i') = S_i(\beta) \oplus S_i(\beta \oplus \beta') \oplus S_i(0).$$

  - This makes significant part of S_i linear.

DES: Three Rounds

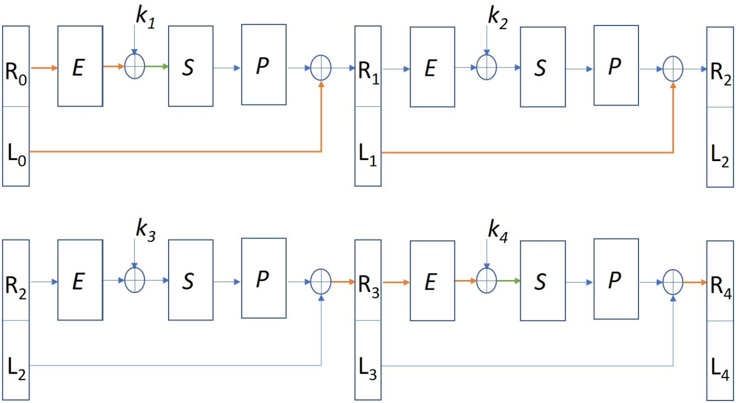
- Such linearity in S_i will render it weak against linearity based attacks.
- Indeed, $|X_i| \leq 16$ for any choice of $\beta_i \oplus \beta'_i$ and $\gamma_i \oplus \gamma'_i$ and any i.
- Therefore, $|K_i| \leq 16$ as per above analysis.
- Doing the same for all S-boxes, we get at most $16^8 = 2^{32}$ possibilities for k_3.
- As before, by repeating the entire process for a few pairs of plaintexts that share right half, we can uniquely identify k_3.
- This is a chosen plaintext attack since plaintext pairs with same right half are required.

DES: Four Rounds



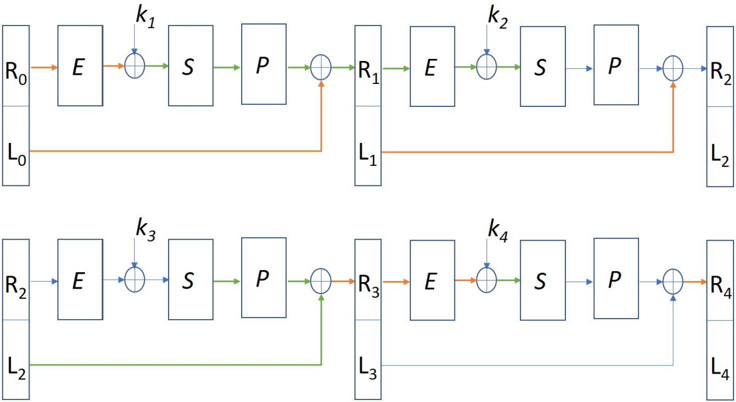
- L_0R_0 is plaintext and L_4R_4 is ciphertext.

DES: Four Rounds



- Texts in all lines marked orange are known.
- Assuming pairs of input text blocks, for lines marked green, XOR is known.

DES: Four Rounds



- Assuming right halves of input pairs to be same, XOR is known for some more lines.

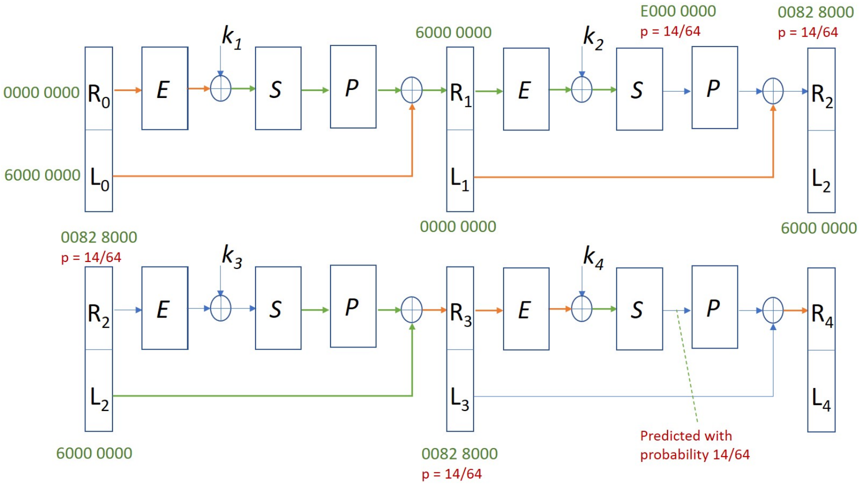
DES: Four Rounds

- There is still no round with known output of E and known XOR of output of S-boxes.
- We know input XOR of second round S-boxes.
- If the output XOR can be predicted, then XOR of R_2 can be predicted, which is same as XOR of L_3.
- This, in turn, gives XOR of output S-boxes of last round.
- We can then use the same method as for three rounds.

DES: Four Rounds

- Since S-boxes are non-linear, fixing input XOR does not fix output XOR.
- So we look for a likely XOR value.
- Examining S1 carefully, we find that if the XOR of two inputs is 001100, then of the 64 possible pairs, 14 result in XOR of the output pair to be 1110.
- If we consider random input pairs that have input XOR to second round S1 as 001100, then we expect that with probability $14/64$, the XOR of the output will be 1110.
- Ensuring that input XOR to remaining S-boxes in second round is all zeroes, we can predict the XOR of the second round output of S-boxes with probability $14/64$.
- We will use hexadecimal notation to represent 32-bit values.

DES: Four Rounds



- We can now repeat the analysis of three round DES.
- It does not work directly though.