CS641

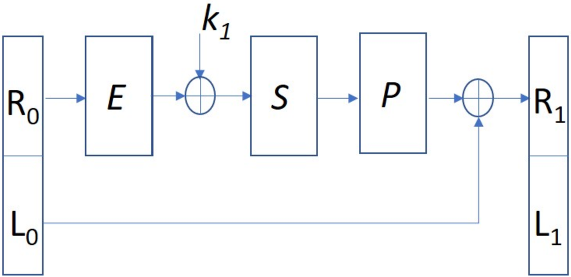
Modern Cryptology

Lecture 5

Approach

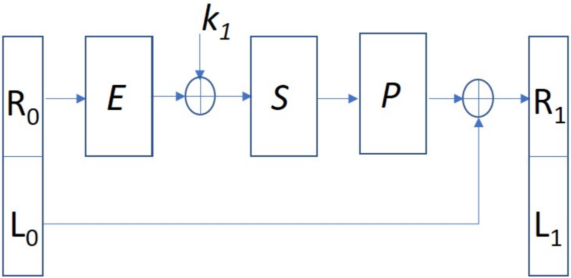
- Brute-force attack to find out the key requires $2^{56} \approx 10^{17}$ operations.
- Frequency analysis based methods do not work at all since variations in frequencies are flattened out by 64 bit blocksize and a sequence of linear transformations.
- We can assume stronger forms of attacks: known-plaintext, chosen plaintext etc.
- We start with easier versions of DES by restricting number of rounds.

DES: One Round



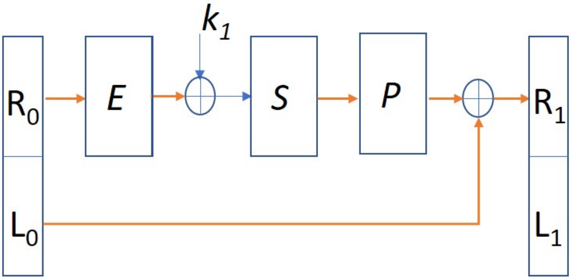
- $L0R_0$ is plaintext and L_1R_1 is ciphertext.
- Since $L_1 = R_0$, half of plaintext is visible in ciphertext, so security already compromised.
- Under a known-plaintext attack, it can be completely broken.

DES: One Round



- Plaintext goes through multiple transformations during encryption.
- Let us analyze which of these transformed texts can be computed when both plaintext and ciphertext are known.

DES: One Round



- Texts in all lines marked orange are known.
- In particular, we know the output of S-boxes as well as output of Expansion.

DES: One Round

- Let $E(R_0) = \alpha_1\alpha_2\cdots\alpha_8$ with $|\alpha_i| = 6$.
- This gets XORed with key $k_1 = k_{1,1}k_{1,2}\cdots k_{1,8}$ with $|k_{1,i}| = 6$ and $\beta_i = \alpha_i \oplus k_{1,i}$.
- Six bit string β_i is input to ith S-box.
- Let $\gamma_i = S_i(\beta_i)$ with $|\gamma_i| = 4$.
- Each γ_i and α_i is known.

DES: One Round

- Since γ_i is known, we can look up the table for S_i to find out which inputs can produce γ_i as output.
- As already observed, table for each S_i has exactly four occurrences of γ_i.
- Let X_i be the set of inputs to S_i that produce γ_i as output.
- We have: $|X_i| = 4$.
- String $\beta_i \in X_i$.
- Let $K_i = \{\alpha_i \oplus \beta \mid \beta \in X_i\}$.
- Since $k_{1,i} = \alpha_i \oplus \beta_i$, we have $k_{1,i} \in K_i$, and $|K_i| = 4$.

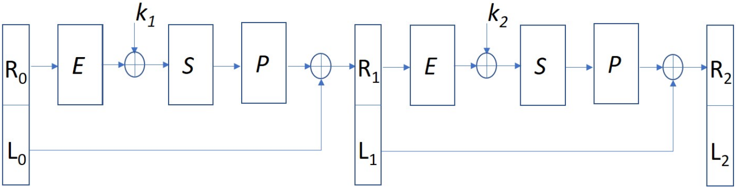
DES: One Round

- Therefore, for every i, $1 \leq i \leq 8$, six bits of k_1 are in the set K_i with $|K_i| = 4$.
- Concatenating strings of K_i, we get $4^8 = 2^{16}$ strings, one of which is k_1.
- This improves on brute-force attack significantly.
- We can do even better!

DES: One Round

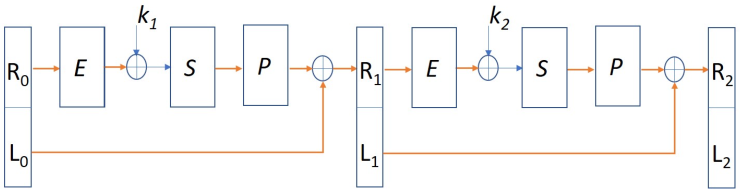
- Take another pair of plaintext and corresponding ciphertext block.
- It is possible under known-plaintext attack.
- Repeat the same analysis as above to get sets K'_i, for $1 \leq i \leq 8$, with $|K'_i| = 4$, and containing six bits of the key k_1.
- Therefore, $K_i \cap K'_i$ also contains six bits of k_1.
- It is likely that size of $K \cap K'_i$ is already one, uniquely identifying part of k_1.
- If it is not unique, do the same exercise with another pair of plaintext-ciphertext block to further reduce the size.
- Once all sets have size 1, the entire key k_1 is uniquely identified.

DES: Two Rounds



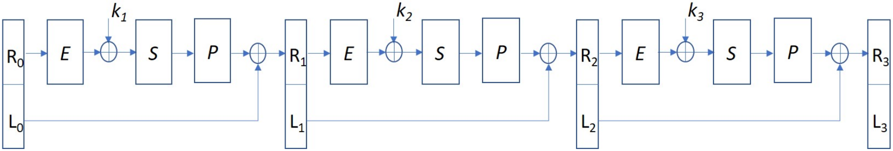
- $L_0 R_0$ is plaintext and $L_2 R_2$ is ciphertext.
- Under a known-plaintext attack, the intermediate block $L_1 R_1$ is known since $L_1 = R_0$ and $R_1 = L_2$.
- Parts of plaintext are no longer visible in the output.
- This can be easily broken as well.

DES: Two Rounds



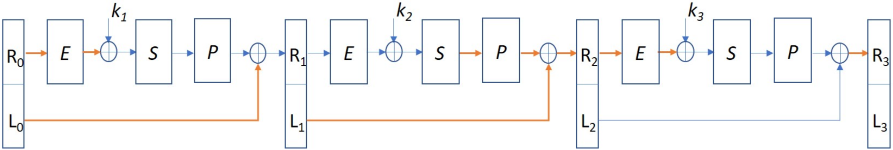
- Texts in all lines marked orange are known.
- In particular, we know the output of S-boxes as well as output of Expansion for both the rounds.
- Using the same strategy as for one round, we can extract key k_1 as well as k_2 easily.

DES: Three Rounds



- $L_0 R_0$ is plaintext and $L_3 R_3$ is ciphertext.

DES: Three Rounds



- Texts in all lines marked orange are known.
- Text $L_2 = R_1$ is not known.
- There is no round for which outputs of both Expansion and S-boxes are known.
- We cannot use the earlier strategy for this.