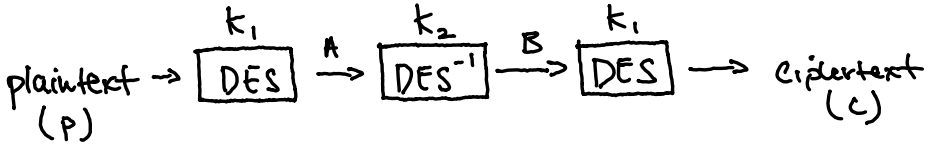
W202 - Homework # 6

Problem 1: Show that you can find K_1 and K_2 with a chosen plaintext attack using 2^{56} chosen plaintexts and two tables of 2^{56} entries of DES inverse operations.

$$3DES = DES_{K_1}\left(DES^{-1}_{K_2}\left(DES_{K_1}(P)\right)\right) = C$$

Answer:

① Let "A" and "B" be intermediate values of the 3DES cryptosystem.



② Using a known plaintext attack, we want to find all plaintext values that result in an intermediate value $A = 0$.

Table # 1: $P_i = DES^{-1}_i(0)$ for $i = 0, 1, 2 \ldots 2^{56}$

P_i	$DES^{-1}_i(0)$
0	$DES^{-1}_0(0)$
1	$DES^{-1}_1(0)$
2	$DES^{-1}_2(0)$
...	...

(2^{56} values)

(next page)

③ For each chosen plaintext P_i, we need to calculate corresponding ciphertext C_i.

Table #2: $C_i = DES_{K1}(DES^{-1}_{K2}(DES_{K1}(P_i)))$ for $i = 0, 1, 2 \ldots 2^{56}$

C_i	$3DES(P_i)$
0	$3DES(P_0)$
1	$3DES(P_1)$
2	$3DES(P_2)$
...	...

(2^{56} values)

④ Next, we need to calculate intermediate B values for each C_i value (from table #2) where $K_1 = i$.

Table #3: $B_i = DES^{-1}_i(C_i)$ for $i = 0, 1, 2 \ldots 2^{56}$

B_i	$DES^{-1}_i(C_i)$
0	$DES^{-1}_0(C_0)$
1	$DES^{-1}_1(C_1)$
2	$DES^{-1}_2(C_2)$
...	...

(2^{56} values)

⑤ Finally, after computing values in tables above, we must search table #2 for a value i (P_i) that matches with an i (B_i) value from table #3. Matching values indicate a candidate K_1 and K_2 value, respectively. You must test keys by encrypting known plaintext, then decrypting the encryption to confirm key values.

Problem 2:

Is super one-time pad encryption perfectly secure?

$$C = m \oplus k \oplus k^R$$

Answer: The super one-time pad is no longer perfectly secure, and will leak information due to the additional "xor" with key reversal operation. As an example, although keys are randomly generated, there are a number of key values, when reversed and "xor" with key, that can produce a ciphertext equal to plaintext. (see below)

Example:

message : 1011 0010
key : 1001 1001
key^R : 1001 1001

} randomly generated *

Encryption:

1011 0010	message
1001 1001	xor with k
0010 1011	
1001 1001	xor with k^R
1011 0010	ciphertext

message = ciphertext

Summary: In the example above, we showed how certain key values, when "xor" with its reverse, produces ciphertext that is equal to plaintext (leaking information). This pattern is observed from many other keys such as 1111 1111, 0000 0000, 1000 0001, etc.).

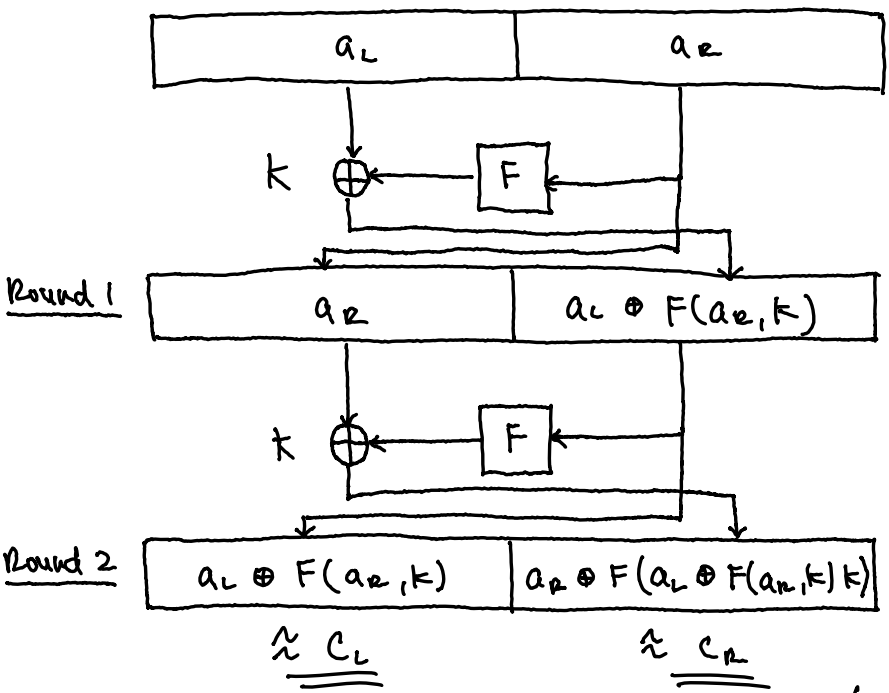
Problem 3: Consider what happens when we run two Feistel cipher rounds on input a and two rounds on input b:

$$(C_L, C_R) = F(F(a_L, a_R))$$
$$(d_L, d_R) = F(F(b_L, b_R))$$

if $F(a_L, a_R) = (a_R, a_L \oplus F(a_R, k))$
(a_L, a_R) and (b_L, b_R) are plaintext pairs
and $a_R, b_R = 0$; $C_L = d_L$
show: $C_R \oplus d_R = 0$

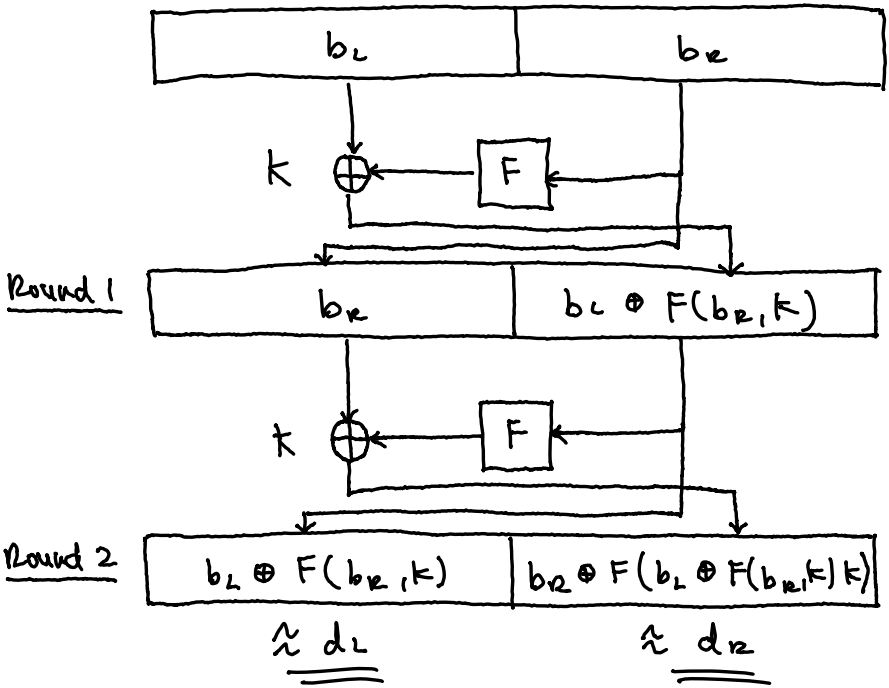
Solution:

① Construct Feistel Cipher diagram (2 rounds) for equation $(C_L, C_R) = F(F(a_L, a_R))$



(next page)

② Construct Feistel Cipher diagram (2 rounds) for equation $(d_L, d_R) = F(F(b_L, b_R))$



③ Given $C_L = d_L$:

$$(a_L \oplus F(a_R, K)) = (b_L \oplus F(b_R, K))$$

* see table # 1 * see table # 2

thus (d_L, d_R) can also be written as :

$$(a_L \oplus F(a_R, K)), (b_R \oplus F(a_L \oplus F(a_R, K), K))$$

Replaced $(b_L \oplus F(b_R, K))$ with $(a_L \oplus F(a_R, K)$ given $C_L = d_R$.

(next page)

④ Based on substitution in step 3, we can compute equation below to show that $C_R \oplus d_R = a_R \oplus b_R = g$:

Step 1 : Compute $C_R \oplus d_R$

$$\underbrace{\left(a_R \oplus F(a_L \oplus F(a_R, k)\, k)\right)}_{C_R} \oplus \underbrace{\left(b_R \oplus F(a_L \oplus F(a_R, k)\, k)\right)}_{d_R}$$

Step 2 : Simplify terms

When an "xor" operation is performed on itself (ie $\left(F(a_L \oplus F(a_R, k)\, k)\right) \oplus \left(F(a_L \oplus F(a_R, k)\, k)\right)$), the result is 0, thus canceling out the terms in the equation. As such, the above equation can be simplified as follows :

$$\left(a_R \oplus \cancel{F(a_L \oplus F(a_R, k)\, k)}\right) \oplus \left(b_R \oplus \cancel{F(a_L \oplus F(a_R, k)\, k)}\right)$$

$$\approx (a_R) \oplus (b_R)$$

Step 3 : Conclusion

As $C_R \oplus d_R$ reduces to $a_R \oplus b_R$, and $a_R \oplus b_R = g$, then $C_R \oplus d_R = g$.

References

Student Discussions

- Eduard Kotysh
- Aaron Crouch
- Matthew Holmes

} Office hours (Slack

Tools and Resources

- Hoffstein textbook
- Stallings textbook
- Async video (module 7)
- Google searches
- Youtube
- Wikipedia
- Stack Exchange