LASEC
SECURITY AND CRYPTOGRAPHY LABORATORY

EPFL / I & C
CH-1015 Lausanne
Phone: ++41 (0) 21 693 76 03
Fax: ++41 (0) 21 693 68 79
URL: http://lasecwww.epfl.ch

Midterm Solution

1 Attacking a Block Cipher by Introducing Faults

1. A decryption algorithm for E exists if and only if all functions T_i, $1 \leq i \leq \ell$ are invertible, i.e., are some permutations. The decryption algorithm is very similar to the encryption except that the order of the subkeys is inverted and each transformation T_i is replaced by its inverse. The decryption algorithm is depicted in Figure 1.

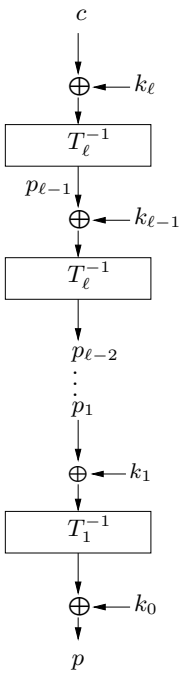

Figure 1: Decryption algorithm of the block cipher E

2. Looking at the round structure of the block cipher E, we directly notice that $c = T(p_{\ell-1}) \oplus k_\ell$ and $c' = T(p_{\ell-1} \oplus \delta) \oplus k_\ell$. Doing a xor operation between these two equations leads to the desired relation
$$c \oplus c' = T(p_{\ell-1}) \oplus T(p_{\ell-1} \oplus \delta).$$

3. Yes, it is possible. To this, it suffices to notice that producing faults on $p_{\ell-1}$ has exactly the same effect as producing the same faults on the subkey $k_{\ell-1}$. Namely, the ciphertext c' is unchanged since $p'_{\ell-1} = p_{\ell-1} \oplus \delta = T(p_{\ell-2}) \oplus k_{\ell-1} \oplus \delta$.

4. An element $x \in \{0,1\}^n$ is a candidate for $p_{\ell-1}$ if and only if there exists a subkey $k_\ell \in \{0,1\}^n$ such that $T(x) \oplus k_\ell = c$ and $T(\delta \oplus x) \oplus k_\ell = c'$. This is equivalent for x to satisfy $T(x) \oplus T(\delta \oplus x) = c \oplus c'$. For showing this equivalence, it suffices to set $k_\ell := T(x) \oplus c$ and use the fact that k_ℓ can take all possible values in $\{0,1\}^n$ since it is uniformly distributed in $\{0,1\}^n$. From the above discussion, we obtain a criterion for deciding whether an element $x \in \{0,1\}^n$ is a candidate for p_ℓ, i.e., checking that $T(x) \oplus T(\delta \oplus x) = c \oplus c'$. In this exercise, $c \oplus c' = (010, 000, 000, 000)$, which immediately implies that the 9 last bits of p_ℓ can be anything. From the following table,

x	$x \oplus 001$	$f(x) \oplus f(x \oplus 001)$
000	001	001
001	000	001
010	011	101
011	010	101
100	101	110
101	100	110
110	111	010
111	110	010

we obtain that the candidates for $p_{\ell-1}$ are of the form $(11*, ***, ***, ***)$, where the symbol $*$ can be replaced by any bit. In total, this leads to 2^{10} candidates.

5. In this question, we had to note that each candidate for $p_{\ell-1}$ defines a unique candidate for k_ℓ which corresponds to $c \oplus T(p_{\ell-1})$. Thus, the number of candidate values for k_ℓ is 2^{10} as well.

6. By definition, $\mathrm{DP}^T(\delta, \delta') = \Pr_{x \in_U \{0,1\}^{12}}[T(x) \oplus T(x \oplus \delta) = \delta')]$, which is equal to

$$\frac{\#\{x \in \{0,1\}^{12} \mid T(x) \oplus T(x \oplus \delta) = \delta')\}}{2^{12}} = \frac{2^{10}}{2^{12}} = 2^{-2}.$$

7. This works similarly as the previous question except that we replace 12 by n. We also note that N_ℓ is the cardinality of the set $\{x \in \{0,1\}^n \mid T(x) \oplus T(x \oplus \delta) = \delta'\}$, which allows to conclude that

$$N_\ell = 2^n \cdot \mathrm{DP}^T(\delta, \delta').$$

8. From the experiment, we trivially know that there exists at least one candidate x for k_ℓ and equivalently for $p_{\ell-1}$. Furthermore, we know that $x \oplus \delta$ is another candidate for $p_{\ell-1}$ since $\delta \neq 0$. Therefore, we always have at least 2 candidates for k_ℓ. Note that this property directly follows from the fact that DP^T is greater or equal than 2^{-n+1} or is equal to zero for any transformation $T : \{0,1\}^n \to \{0,1\}^n$.

9. Since $c \oplus c' = (000, 000, 100, 000)$, the fault occured between the 7th and 9th position. Otherwise, the third block of 3 bits of $c \oplus c'$ would be equal to 000 by definition of T. Now, we look for the elements $x \in \{0,1\}^3$ such that $f(x) \oplus f(x \oplus \Delta) = 100$ for a bitstring $\Delta \in \{001, 010, 100\}$. This corresponds to the bitstrings 001, 101, 011, 111, all with the same $\Delta = 100$. Hence, the candidates for $p_{\ell-1}$ are of the form $(***, ***, y, ***)$ where y is an arbitrary element of $\{001, 101, 011, 111\}$. This leads to 2^{11} candidates for k_ℓ.