Math 116 Homework 7

Jerry Liu, 404474229

March 10, 2016

Book Problems

Chapter 4

Problem. 1.

Part. a.

Solution.
Given M_jM_{j+1}, the output is $M_{j+1}M_{j+2}$. For all j, let $L_j = M_j$ and $R_j = M_{j+1}$.
It is clear that the encryption process is identical to that of DES
except the key used in function $f(K, M_j)$ is always the same. Given ciphertext M_mM_{m+1}:

1. Switch M_m and M_{m+1} to get $M_{m+1}M_m$
2. Do the same encryption process
3. After m rounds, we get M_1M_0, switch back to get M_0M_1

This works because for the first round: we get

$$M_m[M_{m+1} \oplus f(K, M_m)] = M_m[M_{m-1} \oplus f(K, M_m) \oplus f(K, M_m)] = M_mM_{m-1}$$

For a generic step $0 < j < m$, given ciphertext $M_{j+1}M_j$

$$M_j[M_{j+1} \oplus f(K, M_j)] = M_j[M_{j-1} \oplus f(K, M_j) \oplus f(K, M_j)] = M_jM_{j-1}$$

After m steps, we would get M_1M_0, apply step (3) to get the plaintext. □

Part. b.

Solution.
Start with M_0, M_1

1. $M_1M_2 = M_1[M_0 \oplus f(K, M_0)] = M_1[M_0 \oplus f(K, M_1)] = M_1[M_0 \oplus M_1 \oplus K]$
2. $M_2M_3 = [M_0 \oplus M_1 \oplus K][M_1 \oplus f(K, M_2)] = [M_0 \oplus M_1 \oplus K][M_1 \oplus M_2 \oplus K]$

If we XOR M_2 and M_3, we get $M_0 \oplus M_2$, then we XOR the result with M_2 to get M_0. If we have the plaintext, we know M_1, we can XOR M_2 with $M_0 \oplus M_1$ to get the key K.

Part. c.

Proof.
For the 3^{rd} round:

$$M_3 = M_1 \oplus f(K, M_2) = M_1 \oplus M_2 \oplus K = M_1 \oplus M_0 \oplus M_1 \oplus K \oplus K = M_0$$
$$M_4 = M_2 \oplus f(K, M_3) = M_2 \oplus M_3 \oplus K = M_0 \oplus M_1 \oplus K \oplus M_0 \oplus K = M_1$$

As we can see, the third round produces the plaintext, and thus it is insecure. □

Problem. 8.

Proof.
We know the encryption process is given by:

$$L_i = R_{i-1}, \qquad M_i = L_{i-1}, \qquad R_i = f(K_i, R_{i-1}) \oplus M_{i-1}$$

Change symbols $L \to A,\ M \to B,\ R \to C$, and change the order:

$$C_{i-1} = A_i, \qquad A_{i-1} = B_i, \qquad f(K_i, C_{i-1}) \oplus B_{i-1} = C_i$$

XOR both sides by $f(K_i, C_{i-1})$, we get:

$$A_{i-1} = B_i, \qquad f(K_i, C_{i-1}) \oplus f(K_i, C_{i-1}) \oplus B_{i-1} = f(K_i, C_{i-1}) \oplus C_i, \qquad C_{i-1} = A_i$$

Notice $C_{i-1} = A_i$, so we substitute C_{i-1} in the function $f(K_i, C_{i-1})$ by A_i:

$$A_{i-1} = B_i, \qquad B_{i-1} = f(K_i, A_i) \oplus C_i, \qquad C_{i-1} = A_i$$

And this is exactly the decryption algorithm described in the problem. □

Problem. 10.

Solution.
Suppose C_j is transferred incorrectly and becomes C'_j. Since the decryption goes by $P_i = D_K(C_i) \oplus C_{i-1}$, the *only* two plaintext blocks affected will be $P_j = D_K(C'_j) \oplus C_{j-1}$ and $P_{j+1} = D_K(C_{j+1}) \oplus C'_j$.

Chapter 5

Problem. 3. Note: in $GF(2^8)$ addition is XOR.

Part. a.

Proof.
Pick arbitrary $\alpha, \beta, x_1, x_2, x_3, x_4 \in GF(2^8)$ such that $x_1 \oplus x_2 = x_3 \oplus x_4$. Let $f(x_i) = \alpha x_i + \beta$.

$$f(x_1) \oplus f(x_2) = f(x_1) + f(x_2) = (\alpha x_1 + \beta) + (\alpha x_2 + \beta)$$
$$f(x_3) \oplus f(x_4) = f(x_3) + f(x_4) = (\alpha x_3 + \beta) + (\alpha x_4 + \beta)$$

Since we are working in a finite field $GF(2^8)$, we can apply distributivity and associativity:

$$f(x_1) \oplus f(x_2) = (\alpha x_1 + \beta) + (\alpha x_2 + \beta) = \alpha(x_1 + x_2) + 2\beta = \alpha(x_1 \oplus x_2) + 2\beta$$
$$f(x_3) \oplus f(x_4) = (\alpha x_3 + \beta) + (\alpha x_4 + \beta) = \alpha(x_3 + x_4) + 2\beta = \alpha(x_3 \oplus x_4) + 2\beta$$

Since we know $x_1 \oplus x_2 = x_3 \oplus x_4$,

$$f(x_1) \oplus f(x_2) = \alpha(x_1 \oplus x_2) + 2\beta = \alpha(x_3 \oplus x_4) + 2\beta = f(x_3) \oplus f(x_4)$$

□

Part. b.

Proof.
We will prove that ShiftRow, MixColumn and RoundKey satisfy the property.

ShiftRow Transformation Since it cyclicly shifts each row to the left by an offset of 1, 2, and 3, for any two elements in $GF(2^8)$, each entry of one element has the same location in the matrix as another element's entry after transformation. So it does not change the relationship beforehand. Thus it satisfies equal difference property.

MixColumn Transformation Let $f(x) = Mx$, where x is a binary string in matrix form, and M is the MixColumn Transformation. By properties of linear transformation, if $x_1 \oplus x_2 = x_3 \oplus x_4$ for some $x_1, x_2, x_3, x_4 \in GF(2^8)$, apply transformation matrix M to both sides:

$$\begin{aligned}
&M(x_1 \oplus x_2) = M(x_3 \oplus x_4)\\
\Leftrightarrow &M(x_1 + x_2) = M(x_3 + x_4)\\
\Leftrightarrow &Mx_1 + Mx_2 = Mx_3 + Mx_4\\
\Leftrightarrow &f(x_1) + f(x_2) = f(x_3) + f(x_4)\\
\Leftrightarrow &f(x_1) \oplus f(x_2) = f(x_3) \oplus f(x_4)
\end{aligned}$$

$\Rightarrow$ MixColumn Transformation has equal difference property.

RoundKey Addition $f(x) = x \oplus K$, where K is the round key and x is an element in $GF(2^8)$. If $x_1 \oplus x_2 = x_3 \oplus x_4$ for some $x_1, x_2, x_3, x_4 \in GF(2^8)$,

$$\begin{aligned}
f(x_1) \oplus f(x_2) &= x_1 \oplus K \oplus x_2 \oplus K && \text{By distributivity}\\
\Rightarrow f(x_1) \oplus f(x_2) &= x_1 \oplus x_2 \oplus K \oplus K\\
&= x_1 \oplus x_2
\end{aligned}$$

Similarly, $f(x_3) \oplus f(x_4) = x_3 \oplus x_4$. $\Rightarrow f(x_1) \oplus f(x_2) = f(x_3) \oplus f(x_4)$.
So RoundKey Addition also satisfies equal difference property. □

Problem. 4.

Part. a.

Proof.
It suffices to show that if functions f and g satisfy the equal difference property, then the composite $f \circ g$ also has this property. Since all transformations except the ByteSub one have this property, then the AES with ByteSub removed will have this property. □

Part. b.

Proof.
Since ShiftRow and MixColumn transformations are fixed and independent of the key,
let $s =$ ShiftRow and $m =$ MixColumn.
By part a, $E = m \circ s$ has the equal difference property.
Since m is a linear transformation, $m(s(x_1) + s(x_2)) = m(s(x_1)) + m(s(x_2))$.
Let $x_3 = x_1 + x_2$ and $x_4 = 0$,

$$\begin{aligned} & s(x_1) + s(x_2) = s(x_3) + s(x_4) = s(x_1 + x_2) \\ \Leftrightarrow\ & m(s(x_1 + x_2)) = m(s(x_1)) + m(s(x_2)) \\ \Leftrightarrow\ & E(x_1) \oplus E(x_2) = E(x_1 \oplus x_2) = m \circ s(x_1 \oplus x_2) \end{aligned}$$

Since m and s are fixed and do not involve the key,
the result of the transformation E is independent of the key. □

Part. c.

Solution.
Let E' be the transformation in part b, let $E = E' \oplus K$, where K is the round key.
Note: by part b, $E'(x_1) \oplus E'(x_2) = E'(x_1 \oplus x_2)$.
Eve can easily do:

1. Let x_1 go through the process of ShiftRow and MixColumn step, get $E'(x_1)$
2. XOR $E'(x_1)$ with $E(x_1)$ and get round key K.
3. XOR $E(x_2)$ with key K and get $E'(x_2)$.
4. XOR $E'(x_1)$ and $E'(x_2)$ and get $E'(x_1 \oplus x_2)$.
5. Invert $E'(x_1 \oplus x_2)$ by E'^{-1} and get $x_1 \oplus x_2$.
6. XOR $x_1 \oplus x_2$ with x_1 to get x_2.

That's how Eve decrypts x_2

Chapter 8

Problem. 1.

Solution.
By Fermat's theorem, $\alpha^{p-1} \equiv 1 \pmod p$, so we can easily get collisions: $h(x) = h(x + p - 1)$

Problem. 3.

Solution.
Property:

1. Satisfied. XOR is very fast
2. Not satisfied. If $m = x \mid\mid 1 \mid\mid 1 \mid\mid 1 \mid\mid \ldots$, and the number of 1s is even, then $h(m) = m$.
3. Not satisfied. The message $m' = M_l \mid\mid \ldots \mid\mid M_2 \mid\mid M_1$ will collide with m