Solutions 2

CSC 152/252 – Cryptography

Please notify me of any errors you find. If you need help, ask.

1) *Let's say that the key used with AES-128 is* `0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F`*. Compute the first two round keys used by AES-128 in this case (ie, compute k_0 and k_1 in Fig 4.2 which is also $W[0]$ through $W[7]$ in the Fig 4.5).*

The first round key is just the key supplied by the user. The second round key can be computed following Fig 4.5 from the reading.

$$
\begin{aligned}
W[4] &= W[0] \oplus g(W[3]) \\
&= W[0] \oplus g(\texttt{0x0C}, \texttt{0x0D}, \texttt{0x0E}, \texttt{0x0F}) \\
&= W[0] \oplus (S(\texttt{0x0D}) \oplus 1, S(\texttt{0x0E}), S(\texttt{0x0F}), S(\texttt{0x0C})) \\
&= W[0] \oplus (\texttt{0xD6}, \texttt{0xAB}, \texttt{0x76}, \texttt{0xFE}) \\
&= (\texttt{0x00}, \texttt{0x01}, \texttt{0x02}, \texttt{0x03}) \oplus (\texttt{0xD6}, \texttt{0xAB}, \texttt{0x76}, \texttt{0xFE}) \\
&= (\texttt{0xD6}, \texttt{0xAA}, \texttt{0x74}, \texttt{0xFD})
\end{aligned}
$$

Once you have $W[4]$ the rest are easy: $W[5] = W[4] \oplus W[1]$, $W[6] = W[5] \oplus W[2]$, and $W[7] = W[6] \oplus W[3]$.

2) *Using the k_0 and k_1 computed in Problem 1, what is the value of the evolving AES block after "round 1" in Fig 4.2 if initially the AES block ("plaintext x" in Fig 4.2) is* `0xFF, 0xFE, 0xFD, 0xFC, 0xFB, 0xFA, 0xF9, 0xF8, 0xF7, 0xF6, 0xF5, 0xF4, 0xF3, 0xF2, 0xF1, 0xF0`

After the first KeyAddition, the block is the byte `0xFF` repeated 16 times. After the first ByteSubstitution, the block is the byte `0x16` repeated 16 times. After the first ShiftRows, the block is the byte `0x16` repeated 16 times. For MixColumns, you could do all the multiplications and then the additions but you could also use the distributive property and factor out the common term, $2 \cdot \texttt{0x16} + 3 \cdot \texttt{0x16} + 1 \cdot \texttt{0x16} + 1 \cdot \texttt{0x16} = (2+3+1+1) \cdot \texttt{0x16} = 1 \cdot \texttt{0x16} = \texttt{0x16}$. So, after the first MixColumns, the block is the byte $0x16$ repeated 16 times. So, the solution to this problem is the byte $0x16$ repeated 16 times xor'd with the $(W[4], W[5], W[6], W[7])$ computed in Problem 1. Note that I chose these values to reduce your work, usually all the bytes will look random.

3) *GF(16) is defined like GF(256) except the polynomials all have degree less than 4 and the modulus is $x^4 + x + 1$. Calculate the following, each digit representing a field element in hexadecimal. (a) $5 + F$. (b) $5 - F$. (c) $5 \cdot F$. (d) $5/F$. Note that $5 - F$ is shorthand for $5 + (-F)$ where $-F$ is F's additive inverse, and $5/F$ is shorthand for $5 \cdot (F^{-1})$ where F^{-1} is F's multiplicative inverse.*

(a) $(x^2 + x^0) + (x^3 + x^2 + x^1 + x^0) = x^3 + x^1 = A$, or recognizing that addition is just xor of the coefficients $\texttt{0b0101} \oplus \texttt{0b1111} = \texttt{0b1010} = A$.
(b) $5 - F$ is shorthand for $5 + (-F)$, and $-F$ is the value that when added to F yields 0 (in this case $F + F = 0$, so $-F = F$). So, $5 - F = 5 + (-F) = 5 + F = A$.
(c) $(x^2 + x^0) \cdot (x^3 + x^2 + x^1 + x^0) = x^5 + x^4 + x^1 + x^0$. But, since this is not an element of GF(16), we must reduce it modulo $x^4 + x + 1$. $(x^5 + x^4 + x^1 + x^0)/(x^4 + x + 1)$ gives a quotient of $x + 1$ and a remainder of $x^2 + x$, so the answer is $x^2 + x = 6$.
(d) $5/F$ is shorthand for $5 \cdot F^{-1}$, and F^{-1} is the value that when multiplied by F yields 1. You could brute-force try all 15 candidates until you found the inverse which give us $(x^3 + x^2 + x^1 + x^0)^{-1} = x^3$. So, the answer is $(x^2 + x^0) \cdot (x^3) = x^5 + x^3 = x^3 + x^2 + x$.

P1 & P2) Programming assignments will be discussed in class (or office hours if you'd like).