1. The real AES acts on a $4 \times 4$ state of 16 cells. Of Addkey, MixColumn, Rotbyte, and Bytesub, i) which provide diffusion of plaintext bits within each cell? ii) which provide diffusion of plaintext bit between/across cells? (Some may do both or neither.) (10 points)

Solution. i) MixColumn and Bytesub. ii) MixColumn and Rotbyte.

2. I encoded a digraph using ASCII to get a 16 bit plaintext and encrypted that using SAES and the key $K_0 = 1010 \ 0101 \ 0100 \ 0000$. So $K_1 = 1011 \ 1000 \ 1111 \ 1000$ and $K_2 = 1110 \ 1111 \ 0001 \ 0111$. The ciphertext is 0001 1111 1000 1101. Decryption is given by: $A_{K_0} \circ SR^{-1} \circ NS^{-1} \circ A_{c(z)-1K_1} \circ MC^{-1} \circ SR^{-1} \circ NS^{-1} \circ A_{K_2}$. Bob started decryption and determined that $MC^{-1} \circ SR^{-1} \circ NS^{-1} \circ A_{K_2}(0001 \ 1111 \ 1000 \ 1101) = 0011 \ 1110 \ 0111 \ 0101$. Finish the decryption and decode to sensible plaintext. (20 points)

Solution. $c(z)^{-1}(K_1) = MC^{-1}(K_1) = 1111 \ 0001 \ 1101 \ 1001$

$A_{c(z)-1(K_1)}(0011 \ 1110 \ 0111 \ 0101) = 0011 \ 1110 \ 0111 \ 0101 \oplus 1111 \ 0001 \ 1101 \ 1001 = 1100 \ 1111 \ 1010 \ 1100$

$NS^{-1}(1100 \ 1111 \ 1010 \ 1100) = 1100 \ 1111 \ 0010 \ 1100$

$SR^{-1}(1100 \ 1110 \ 0010 \ 1100) = 1100 \ 1110 \ 0010 \ 1110$

$A_{K_0}(1100 \ 1110 \ 0010 \ 1110) = 1100 \ 1110 \ 0010 \ 1110 \ 1111 \ 0010 \ 0101 \ 0000 = 0110 \ 1001 \ 0110 \ 1110$

3. Alice and Bob are using an affine encryption cipher. So encryption is done by $C \equiv aP + b(mod \ 26)$. Eve has intercepted a fairly short ciphertext. She has found that the most common ciphertext letter is $N \sim 13$ and guesses that is the encryption of $E \sim 4$. She has found that the second most common ciphertext letter is $O \sim 14$ and guesses that is the encryption of $T \sim 19$. The ciphertext starts HMDV ~ . Correctly decrypt HMDV to sensible plaintext. If at first you don’t succeed ... (20 points)

Solution. Eve wants to decrypt. So she wants to find $a’, b’$ in $P \equiv a’C + b’(mod \ 26)$. Guessing that the ciphertext $N \sim 13$ comes from $E \sim 4$ and the ciphertext $O \sim 14$ comes from $T \sim 19$. So she has $4 \equiv a’13 + b’(mod \ 26)$ and $19 \equiv a’14 + b’(mod \ 26)$. Subtracting the first from the second gives $15 \equiv a’(mod \ 26)$. From the first “equation” we have $4 \equiv 15 \cdot 13 + b’(mod \ 26)$ so $b’ \equiv 4 - 15 \cdot 13 \equiv 17(mod \ 26)$. Eve tries $P \equiv 15C + 17(mod \ 26)$ on HMDV and it decrypts to SPKU, which is not sensible. Since there wasn’t much ciphertext, there wasn’t much plaintext. So perhaps T was most common and E was second most common in the plaintext. Eve tries $19 \equiv a’13 + b’(mod \ 26)$ and $4 \equiv a’14 + b’(mod \ 26)$. She subtracts the first from the second and gets $11 \equiv a’(mod \ 26)$. From the first “equation” we have $19 \equiv 11 \cdot 13 + b’(mod \ 26)$ so $b’ \equiv 19 - 11 \cdot 13 \equiv 6(mod \ 26)$. Eve tries $P \equiv 11C + 6(mod \ 26)$ on HMDV and it decrypts to FIND, which is sensible plaintext.

4. We encode the letters A - P with their 4 bit binary representation of their corresponding numbers. So $A = 0000, B = 0001, \ldots, P = 1111$. Alice sends you the ciphertext 01110000 from a modern stream cipher. Here is how the (pseudo)random bit generator works. You and Alice agree on a positive rational number as a key (seed). You and Alice agreed on 9/17 earlier. To get the
keystream, find the decimal representation of \(9/17\) and reduce each digit after the decimal mod 2. Decrypt and decode to sensible plaintext. (20 points)

Solution. \(9/17 = 0.52941176\ldots\) Now 5, 6, 9, 4, 1, 1, 7, 6 \(\equiv 1, 0, 1, 0, 1, 1, 0\) (mod 2). We compute 01110000 \(\oplus\) 10101110 = 1101 1110 \(\sim\) NO.

5. The Kreblachian language has 10000 different letters, which they encode as the integers 0, 1, \ldots, 9999 for an affine encryption cipher. Two silly users agree that they will use \(C \equiv 6P + 2357\) (mod 10000) for encryption. The symbol encoded as the number 19 encrypts to the same ciphertext number as the symbol encoded as what other number (from 0 to 9999)? (20 points)

Solution. We have \(6(19) + 2357 \equiv 6P + 2357\) (mod 10000) or \(6(19) \equiv 6P\) (mod 10000). Since \(\gcd(2, 10000) = 2\) we get \(3(19) \equiv 3P\) (mod 5000). Since 3 is invertible mod 10000, we multiply both sides by \(3^{-1}\) and get \(19 \equiv P\) (mod 5000). There are exactly two numbers from 0, \ldots, 9999 that are \(19\) (mod 5000), namely 19 and 19 + 5000 = 5019. So the other number is 5019.

6. You and Bob are using the Playfair cipher with key UNCOPYRIGHTABLE. Bob sends you the ciphertext DGWBAT. Decrypt to sensible plaintext. (10 points)

\[
\begin{array}{cccc}
U & N & C & O \\
Y & R & IJ & G \\
T & A & B & L \\
D & F & K & M \\
S & V & W & X \\
\end{array}
\]

Solution. The table is

\[
\begin{array}{cccc}
U & N & C & O \\
Y & R & IJ & G \\
T & A & B & L \\
D & F & K & M \\
S & V & W & X \\
\end{array}
\]

We get MY KITE.