№7 Стандарт шифрования AES. Перемножить байты:

① $(1,1,0,1,0,0,1,1)\cdot(0,1,1,1,0,0,1,1)$

② $(0,1,0,1,0,1,0,1)\cdot(1,0,1,0,1,0,1,0)$

① Для того, чтобы найти произведение байтов $(\overset{7}{1},\overset{6}{1},0,\overset{4}{1},0,0,\overset{1}{1},\overset{0}{1})\cdot(0,\overset{6}{1},\overset{5}{1},\overset{4}{1},0,0,\overset{1}{1},\overset{0}{1})$, запишем их в виде многочленов и вычислим вначале умножение в кольце $Z_2[x]$:

$$(x^7+x^6+x^4+x^1+1)\cdot(x^6+x^5+x^4+x^1+1)=$$

$$=(x^{13}+x^{12}+x^{11}+x^8+x^7+x^{12}+x^{11}+x^{10}+x^7+x^6+x^{10}+x^9+x^8+$$
$$+x^5+x^4+x^7+x^6+x^5+x^2+x^1+x^6+x^5+x^4+x^1+1) \bmod 2$$

$$=x^{13}+x^9+x^7+x^6+x^5+x^2+1$$

Затем вычислим остаток при делении полученного многочлена на $f(x)$, где

$f(x)=x^8+x^4+x^3+x^1+1$:

$$\begin{array}{l|l}
\;\; x^{13}+x^9+x^7+x^6+x^5+x^2+1 & x^8+x^4+x^3+x^1+1 \\ \cline{2-2}
-\underline{x^{13}+x^9+x^8+x^6+x^5} \;\; \bmod 2 & \underbrace{x^5+1}_{\text{частное}} \\
\;\; x^8+x^7+x^2+1 & \\
-\underline{x^8+x^4+x^3+x^1+1} \;\; \bmod 2 & \\
\;\; \underbrace{x^7+x^4+x^3+x^2+x}_{\text{остаток}} &
\end{array}$$

Получаем: $x^{13}+x^9+x^7+x^6+x^5+x^2+1=f(x)\cdot(x^5+1)+(x^7+x^4+x^3+x^2+x)$

А, значит, произведением будет байт:

(1, 0, 0, 1, 1, 1, 1, 0)

(2) $(x^6+x^4+x^2+1)\cdot(x^7+x^5+x^3+x^1)=$

$=(x^{13}+x^4+x^9+x^7+x^{11}+x^9+x^7+x^5+x^9+x^7+x^5+x^3+x^7+x^5+$

$+x^3+x^1)\bmod 2 = x^{13}+x^9+x^5+x^1$

$$
\begin{array}{rl|l}
 & x^{13}+x^9+x^5+\cancel{x} & x^8+x^4+x^3+x^1+1 \\
\cline{3-3}
\text{mod 2} & -\;x^{13}+x^9+x^8+x^6+x^5 & x^5+1 \\
\cline{2-2}
 & x^8+x^6+\cancel{x^1} & \\
\text{mod 2} & -\;x^8+x^4+x^3+x^1+1 & \\
\cline{2-2}
 & \underbrace{x^6+x^4+x^3+1} & \Rightarrow (0,1,0,1,1,0,0,1)
\end{array}
$$