

Practice T/F

1. ☒ F Only ECB and CBC require both Enc and Dec boxes but not OFB and CFB.
2. ☒ F Feistel with $f=id$, $(L, R) \rightarrow (R, L \oplus f(L))$
3. ☒ F $ESC^{-1} = ACK$ under AES
 $ESC = 27 = 16 + 8 + 2 + 1 = 11011 = x^4 + x^3 + x + 1$
 $ACK = 6 = 4 + 2 = 110 = x^2 + x$
 $ESC \times ACK = (x^4 + x^3 + x + 1)(x^2 + x) = x^6 + x^5 + x^3 + x^2 + x + 1$
 $\pmod{x^8 + x^4 + x^3 + x + 1}$
4. ☒ F $x^3 + x + 1$ is irreducible
 Try all linear factors: $x \nmid x^3 + x + 1$, $x+1 \nmid x^3 + x + 1$

$$\begin{array}{r} x^2+1 \\ x \overline{) x^3+x+1} \\ \underline{x^3} \\ x+1 \\ \underline{x} \\ 1 \end{array} \quad \begin{array}{r} x^2+x \\ x+1 \overline{) x^3+x+1} \\ \underline{x^3+x^2} \\ x^2+x+1 \\ \underline{x^2+x} \\ 1 \end{array}$$

 no linear divisors $\Rightarrow$ no nontrivial divisors
5. ☒ F Blum Rabin: Alice factors Bob's modulus with prob. $1/2$ (when Bob guesses the wrong square root)
6. ☒ F verifier can demand a proof of the square root by sending $b=0$
7. ☒ F n Blum integer $\Rightarrow$ $n-1 \equiv \begin{cases} -1 \pmod{p} \\ -1 \pmod{q} \end{cases}$
 $n=pq$, primes $p \neq q$
 $p \equiv q \equiv 3 \pmod{4}$
 $\left(\frac{-1}{p}\right) = -1$
 $\left(\frac{-1}{q}\right) = -1$