Question 1:

We'll show that F isn't a secure PRF by showing that there exists a PPT D s.t. $\left|\Pr\left[D^{F_k(\cdot)} = 1\right] - \Pr\left[D^{f(\cdot)} = 1\right]\right|$ isn't negligible, where f is a completely random function from $\{0,1\}^m$ to $\{0,1\}^m$

We'll define the distinguisher D as follows:

Let a be an m-bit long string $a_1, \dots, a_m$ s.t. $a_1 = \cdots = a_m = 0$

Let b be an m-bit long string $b_1, \dots, b_m$ s.t. $b_1 = 1$ and $b_2 = \cdots = b_m = 0$

Let c be an m-bit long string $c_1, \dots, c_m$ s.t. $c_1 = 0$ and $c_2 = \cdots = c_m = 1$

Let d be an m-bit long string $d_1, \dots, d_m$ s.t. $d_1 = \cdots = d_m = 1$

D asks its oracle O 4 queries: $O(a), O(b), O(c), O(d)$

D outputs 1 if and only if $O(a) \oplus O(b) = O(c) \oplus O(d)$

- If $O = F_k$, then $\Pr\left[D^{F_k(\cdot)} = 1\right] = 1$, because in this case it holds that:

$$\begin{aligned} O(a) = F_k(a) = k[1, a_1] \oplus k[2, a_2] \oplus \dots \oplus k[m, a_m] = \\ = k[1,0] \oplus k[2,0] \oplus \dots \oplus k[m,0] \end{aligned}$$

$$\begin{aligned} O(b) = F_k(b) = k[1, b_1] \oplus k[2, b_2] \oplus \dots \oplus k[m, b_m] = \\ = k[1,1] \oplus k[2,0] \oplus \dots \oplus k[m,0] \end{aligned}$$

$$\begin{aligned} O(c) = F_k(c) = k[1, c_1] \oplus k[2, c_2] \oplus \dots \oplus k[m, c_m] = \\ = k[1,0] \oplus k[2,1] \oplus \dots \oplus k[m,1] \end{aligned}$$

$$\begin{aligned} O(d) = F_k(d) = k[1, d_1] \oplus k[2, d_2] \oplus \dots \oplus k[m, d_m] = \\ = k[1,1] \oplus k[2,1] \oplus \dots \oplus k[m,1] \end{aligned}$$

Therefore, $O(a) \oplus O(b) = k[1,0] \oplus k[2,0] \oplus \dots \oplus k[m,0] \oplus k[1,1] \oplus k[2,0] \oplus \dots \oplus k[m,0] = k[1,0] \oplus k[1,1]$
(due to associativity and commutativity of $\oplus$ and the fact that $x \oplus x = 0$ and $0 \oplus x = x$)

Similarly, $O(c) \oplus O(d) = k[1,0] \oplus k[2,1] \oplus \ldots \oplus k[m,1] \oplus k[1,1] \oplus k[2,1] \oplus \ldots \oplus k[m,1] = k[1,0] \oplus k[1,1]$

Thus $O(a) \oplus O(b) = k[1,0] \oplus k[1,1] = O(c) \oplus O(d)$, from which we get that: $\Pr\left[D^{F_k(\cdot)} = 1\right] = \Pr[\, O(a) \oplus O(b) = O(c) \oplus O(d)] = \mathbf{1}$

- If $O = f$ (a completely random function), $\Pr\left[D^{f(\cdot)} = 1\right] = \frac{1}{2^n}$ because in this case it holds that:

$$\begin{aligned} \Pr\left[D^{f(\cdot)} = 1\right] &= \Pr[\, O(a) \oplus O(b) = O(c) \oplus O(d)] =_{*} \\ &= \Pr[O(a) \oplus O(a) \oplus O(b) = O(a) \oplus O(c) \oplus O(d)] = \\ &= \Pr[O(b) = O(a) \oplus O(c) \oplus O(d)] =_{**} \\ &= \Pr[f(b) = O(a) \oplus O(c) \oplus O(d)] = \frac{\mathbf{1}}{\mathbf{2^m}} \end{aligned}$$

(*) – performing $\oplus$ on both sides

(**) – since f is a completely random function, the probability that applying f on some input (b in this case) will yield a specific output ($O(a) \oplus O(c) \oplus O(d)$ in this case) among all the $|\{0,1\}^m| = 2^m$ possible outputs is $\frac{1}{2^m}$

From the above, we get that

$\left|\Pr\left[D^{F_k(\cdot)} = 1\right] - \Pr\left[D^{f(\cdot)} = 1\right]\right| = \left|1 - \frac{1}{2^n}\right|$ which isn't negligible (because for $n \geq 1$ it holds that $1 - \frac{1}{2^n} \geq 1 - \frac{1}{2} = \frac{1}{2} > negl(n)$)

Therefore, the proposed F isn't a secure PRF.

Question 2:

The given MAC scheme is **not** secure. We'll recall the definition of a secure MAC scheme:

Definition:
A MAC scheme Π is secure if for every PPT adversary $\mathcal{A}$ there exists a negligible function $\nu(\cdot)$ such that

$$\Pr\left[\mathrm{MacForge}_{\Pi,\mathcal{A}}(n) = 1\right] \leq \nu(n)$$

$$\mathrm{MacForge}_{\Pi,\mathcal{A}}(n) = \begin{cases} 1, & \text{if } \mathrm{Vrfy}_k(m^*, t^*) = 1 \\ & \text{and } m^* \notin Q \\ 0, & \text{otherwise} \end{cases}$$

Q = Set of all queries asked by $\mathcal{A}$

An attacker can break the security of this MAC scheme in the following way:

The attacker asks the query mmm (the concatenation of m with itself 3 times), where m is a 32-byte block that contains only zeroes, for example. The attacker receives $Mac(k, mmm)$, and forges the tag of the query m by outputing $Mac(k, mmm)$. Notice that the attacker didn't ask the query m before.

The probability of a succesfull forging of the attacker is exactly 1, since:

$$Mac(k, mmm) = F(k, m) \oplus F(k, m) \oplus F(k, m) = F(k, m) = Mac(k, m)$$

Where the 2nd equality is due to $\oplus$ properties (mentioned in the previous question) and the fact that F is a PRF, thus it's deterministic.

Therefore, $\Pr[Mac(k, m) = Mac(k, mmm)] = 1 > negl(n)$ and so the MAC scheme isn't secure.

3) חשב $8^{100001} \bmod 1255$ בעזרת משפט השאריות הסיני ומשפט אוילר:

נבין ב-Z^*_{1255},

נפרק את 1255 לגורמים ראשוניים:

$\cancel{\frac{1255}{2}}$ $\cancel{\frac{1255}{3}}$ $\frac{1255}{5} = 251$

5 ראשוני, 251 ראשוני (ידוע, ניתן לוודא שהוא לא מתחלק באף מס עד 16 - השורש שלו.
ניתן לספר ולבדוק רק ראשוניים עד השורש שלו).

לכן קיים איזומורפיזם

$$Z^*_{1255} \approx Z^*_5 \times Z^*_{251}$$

נעבור בינהם:

$$8^{100001} \bmod 1255 \Leftrightarrow (8 \bmod 5, 8 \bmod 251)^{100001} =$$
$$=(3^{100001} \bmod 5, 8^{100001} \bmod 251)$$

$$3^{100001} \bmod 5 = 3\cdot 3^{100000} \bmod 5 = 3\cdot(3^4)^{\frac{100000}{4}} \bmod 5 \overset{\substack{\text{Modular} \\ \text{Exponentiation} \\ \text{Rule}}}{=} 3\cdot(3^4 \bmod 5)^{\frac{100000}{4}} \bmod 5$$
$$= 3\cdot 1^{\frac{100000}{4}} \bmod 5 = 3\cdot 1 \bmod 5 = 3$$ לפי משפט אוילר!

$$8^{100001} \bmod 251 = 8\cdot 8^{100000} \bmod 251 = 8\cdot(8^{250})^{\frac{100000}{250}} \bmod 251 \overset{\substack{\text{Modular} \\ \text{Exponentiation Rule}}}{=} 8\cdot(8^{250} \bmod 251)^{\frac{100000}{250}} \bmod 251$$
$$= 8\cdot 1^{\frac{100000}{250}} \bmod 251 = 8\cdot 1 \bmod 251 = 8$$ לפי משפט אוילר!

קיבלנו שניתן לכתוב את $8^{100001} \bmod 1255$ כ: $(3,8)$ בהצגה האיזומורפית.

נשאר להמיר את $(3,8)$ ל-Z^*_{1255}:

נחשב את:

$$a\cdot \overset{p}{5} + b\cdot \overset{q}{251} = \gcd(5,251) = 1$$

נמצא את a,b בעזרת אוקלידס המורחב:

$$\gcd(5,251) = \gcd(5,1)\ [1 = 251 - 50\cdot 5] = 1$$

מכאן:

$$1 = \underline{1}\cdot 251 + (\underline{-50})\cdot 5 \Rightarrow a=-50,\ b=1$$

נשתמש ב-CRT:

$$1_p = b\cdot q \bmod 1255 = 1\cdot 251 \bmod 1255 = 251$$
$$1_q = a\cdot p \bmod 1255 = -50\cdot 5 \bmod 1255 = 1005$$

$$8^{100001} \bmod 1255 = 3\cdot 1_p + 8\cdot 1_q \bmod 1255 = 3\cdot 251 + 8\cdot 1005 \bmod 1255$$
$$= 8793 \bmod 1255 = \boxed{8}$$