Solutions to Test 2.

1 a) There is one field of size $8^2 = 2^6$ and one field of size $9^2 = 3^4$. There are no fields of size 100.

b) In $\mathbb{Z}_2[x]$, $x^2+1 = (x+1)^2$ so it is reducible.
In $\mathbb{Z}_3[x]$, x^2+1 has no roots so it is irreducible.

2. a) $\phi(77) = 6 \cdot 10 = 60$

$60 = 8 \cdot 7 + 4$
$7 = 4 + 3$
$4 = 3 + 1$

so by back sub. $1 = 2 \cdot 60 - 17 \cdot 7$

so the deciphering exponent is $-17 \equiv 43 \bmod 60$.

b) To encode $m = 7$, we compute $7^{7} \equiv$ mod 77.

3. The most commonly used primality test is the Miller-Rabin algorithm. It is a probabilistic test which will tell you definitively if a number is composite and with reasonable probability correctly identify if the number is prime. The algorithm works like this:

Pick a number a with $\gcd(a, n) = 1$. Write $n - 1 = 2^k m$ for an odd number m. Compute a sequence $b_0, b_1, \ldots b_k$ s.t. $b_0 \equiv a^m \bmod n$ and $b_{i+1} \equiv b_i^2 \bmod n$ for $i < k$.

If $b_0 \equiv \pm 1 \bmod n$ or if $b_i \equiv -1 \bmod n$ for any i, the algorithm declares n is prime. Otherwise it says n is composite. It will always be correct if it says composite and will be correct at least 75% of the time if it says prime.

To increase the chances of being correct if prime is returned, typically one runs the algorithm for several randomly chosen a.

4. From the question,

$$\left(\underbrace{880525 \times 2057202 \times 648581}_{A}\right)^2 \equiv 2 \cdot 6 \cdot 3 = 6^2 \bmod 2288233$$

We also have $A \equiv 720341 \bmod 2288233$

So $A^2 \equiv 6^2 \bmod 2288233$ and $A \neq \pm 6$ so

$\gcd(2288233, 720341 - 6)$ divides 2288233

With a calculator, compute the gcd:

$2288233 - 3 \cdot 720335 = 127228$

$720335 - 5 \cdot 127228 = 84195$

$127228 - 84195 = 43033$

$84195 - 43033 = 1871$

and $1871 \mid 43033$

So $2288233 = 1871 \times 1223$.

You could have also similarly calculated $\gcd(2288233, 720347)$ and got 1223.

5. Suppose F is finite and consider the sequence $1, 1+1, 1+1+1, \ldots$ where we write $k \cdot 1$ for $\underbrace{1+1+\cdots 1}_{k \text{ times}}$.

Since F is finite, for some $k < l$, $k \cdot 1 = l \cdot 1$. But then $(l-k) \cdot 1 = 0$. So there is some m s.t. $m \cdot 1 = 0$. Choose the least such m and suppose $m = k \cdot l$ where $1 < k, l < m$ i.e. suppose m is composite.

Compute $(k \cdot 1) \cdot (l \cdot 1) = \underbrace{(1+\cdots+1)}_{k}\underbrace{(1+\cdots+1)}_{l}$

$$= \underbrace{\underbrace{(1+\cdots+1)}_{l} + \underbrace{(1+\cdots+1)}_{l} \cdots \underbrace{(1+\cdots+1)}_{l}}_{k \text{ times}}$$

$$= m \cdot 1 = 0$$

So $k \cdot 1 = 0$ or $l \cdot 1 = 0$ since F is a field. $\not\downarrow$. contradicts the minimality of m. So m is prime.