Student Number: [redacted] Name: Bryan Hoang

7. (10 points)

(a) **Answer:**

Since $A \equiv 2^{947} \equiv 177 \pmod{1373}$, the value of Alice's public key is $\boxed{A = 177}$.

(b) **Answer:**

Since $c_1 \equiv 2^{877} \equiv 719 \pmod{1373}$ and $c_2 \equiv 583 \cdot 469^{877} \equiv 623 \pmod{1373}$, the ciphertext Alice sends to Bob is $\boxed{(c_1, c_2) = (719, 623)}$.

(c) **Answer:**

Decrypting the message yields

$$(c_1^a)^{-1} \cdot c_2 \equiv (661^{299})^{-1} \cdot 1325 \equiv 645^{-1} \cdot 1325 \equiv 794 \cdot 1325 \equiv 332 \pmod{1373}.$$

Thus, the decrypted message is $\boxed{m = 332}$.

(d) **Answer:**

The solution to the discrete logarithm problem $2^b \equiv 893 \pmod{1373}$ that Eve wants to sovle is $\boxed{b = 219}$. Now that we have Bob's private key, decrypting the message yields

$$(c_1^a)^{-1} \cdot c_2 \equiv (693^{219})^{-1} \cdot 793 \equiv 431^{-1} \cdot 793 \equiv 532 \cdot 793 \equiv 365 \pmod{1373}.$$

Therefore, the message Alice sent to Bob is $\boxed{m = 365}$.