2.6:
We start out with p=1373 g=2 (a primitive root). So Alice has computed: ga ≡ 974 (mod 1373).

Bob would like to use 871 as his secret exponent so that B ≡ gb (mod 1373).
To get the shared key, we need gab

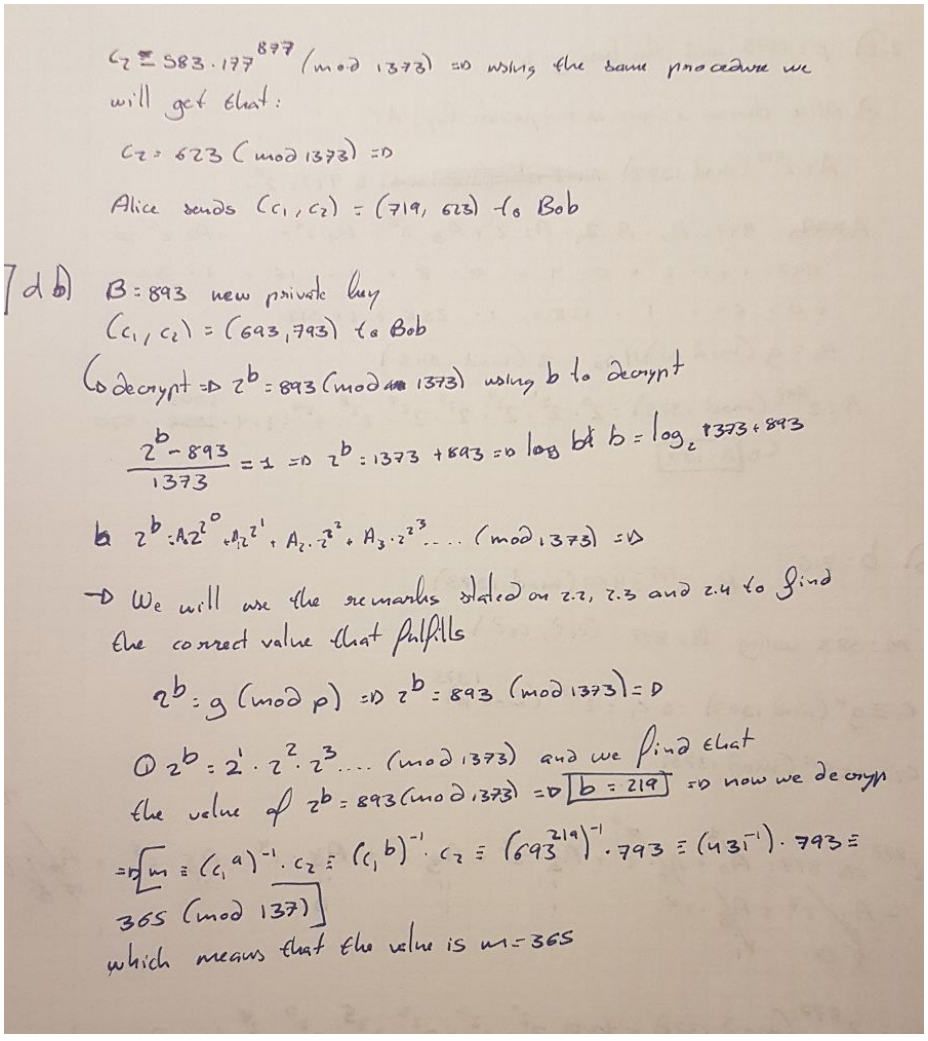
So we first compute 2871 mod 1373 which equals 805
Then compute 974871 mod 1373 which equals 397

[Bob should send alice 805 (mod 1373).]

Now that Bob knows that gab ≡ Ab ≡ 397 (mod 1373) he can find Alice's secret component.
This can be found using discrete logs.

[If ga ≡ 974 (mod 1373) we can use 805587 (mod 1373) which equals 397.]

2.8



$\equiv 2 \pmod{1373}$ ~~(mod 1373)~~ $\Rightarrow 947 \equiv 2^0$.

$A = A_0$ $947 = A_0 \cdot A_1 2_1 + A_2 \cdot 2^2 + A_3 \cdot 2^3 + A_4 \cdot 2^4 + \dots + A_9 \cdot 2^9$

$947 = 1 + 1 \cdot 2 + 0 \cdot 4 + 0 \cdot 8 + 1 \cdot 16 + 1 \cdot 32$

$+ 0 \cdot 64 + 1 \cdot 128 + 1 \cdot 256 + 1 \cdot 512$

$a_0 = g \pmod N$ // $a_0 = 2 \pmod{1373}$

$2.47e+38$ $A = 2^{947} \pmod{1373} = 2^0 \cdot 2^1 \cdot 2^2 \cdot 2^3 \cdot 2^4 \cdot 2^7 \cdot 2^8 \cdot 2^9 = 1 \cdot 4 \cdot$ ~~1005~~ $\cdot 870 \cdot$

$\Rightarrow$ $A = 177$

2.8 b) $b = 916$

$B = 2^{916} \equiv 469 \pmod{1373}$

$m = 583$ using $k = 877$ (c_1?, c_2?)

$c_1 \equiv g^k \pmod{1373} \Rightarrow c_1 = 2^{877} \pmod{1373}$

$c_2 = mA^k \pmod{1373}$

$2^{877} \Rightarrow 877 = A_0 \cdot 2^0 + A_1 \cdot 2^1 + A_2 \cdot 2^2 + A_3 \cdot 2^3 + A_4 \cdot 2^4 + A_5 \cdot 2^5 + A_6 \cdot 2^6$
$+ A_7 \cdot 2^7 + A_8 \cdot 2^8$

$c_1 = 2^{877} \pmod{1373} = 2^0 \cdot 2^2 \cdot 2^3 \cdot 2^5 \cdot 2^7 \cdot 2^8 \pmod{1373}$

$\Rightarrow c_1 = 2^1 \cdot 16 \cdot 256 \cdot 870 \cdot 209 \cdot 1118 \pmod{1373} \Rightarrow c_1 = 1018 \pmod{1373}$

$2^9 = 128$: $\Rightarrow c_1 = 2 \cdot 16 \cdot 256 \cdot 870 \cdot 377 \cdot 1118 \cdot 209 \Rightarrow$

$c_1 = 719 \pmod{1373}$

Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications.

a) Alice chooses $a = 947$ as her private key. What is her public key A?

$A = 2^{947} \bmod 1373$

$947 = 1 + 2 \cdot 473$
$= 1 + 2 + 2 \cdot 472$
$= 1 + 2 + 2 \cdot 2 \cdot 236$
$= 1 + 2 + 2 \cdot 2 \cdot 2 \cdot 118$
$= 1 + 2 + 2 \cdot 2 \cdot 2 \cdot 2 \cdot 59$
$= 1 + 2 + 2 \cdot 2 \cdot 2 \cdot 2 + 2 \cdot 2 \cdot 2 \cdot 2 \cdot 58$
$= 1 + 2 + 2 \cdot 2 \cdot 2 \cdot 2 + 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 29$
$= 1 + 2 + 2^4 + 2^5 + 2^5 \cdot 28$
$= 1 + 2 + 2^4 + 2^5 + 2^6 \cdot 14$
$= 1 + 2 + 2^4 + 2^5 + 2^7 \cdot 7$

$2^{947} = (2^1)(2^2)(2^{16})(2^{32})(2^{14})^{64}$

$2^{947} = (2^1)(2^2)(2^{16})(2^{32})(((((((2^{14})^2)^2)^2)^2)^2)^2)^2)$

Let $x = 2^1 \cdot 2^2 \cdot 2^{16} \cdot 2^{32}$

$2^{947} \bmod 1373 = (x \bmod 1373)(((((((((2^{14})^2)^2)^2)^2)^2)^2)^2) \bmod 1373) \bmod 1373$

$(((((((2^{14} \bmod 1373)^2 \bmod 1373)^2 \bmod 1373)^2 \bmod 1373)^2 \bmod 1373)^2 \bmod 1373)^2 \bmod 1373)$
(226)

$(((((((1281)^2 \bmod 1373)^2 \rightarrow$

$1281^2 \bmod 1373 = 226$

$(226)^2 \bmod 1373)^2 \bmod 1373)^2 \bmod 1373)^2 \bmod 1373)^2 \bmod 1373) \bmod 1373$
275 110 1116 145 430 430

$2^{947} \bmod 1373 = (x \bmod 1373)(430) \bmod 1373$

$= (((2^1)^5(2^2)(2^{16})(2^{32}) \bmod 1373)(430)) \bmod 1373$

~~$(8 \bmod 1373)(2^{16} \bmod 1373)(2^{32} \bmod 1373$~~

$y = (2^3)(2^{16})$

$(y \bmod 1373)(2^{32} \bmod 1373) \bmod 1373 = 738$
1175 870

$(8 \bmod 1373)(2^{16} \bmod 1373) \bmod 1373 = 1175$
8 1005

80...

$(738)(430) \bmod 1373 = 177$

$A = 177$

2.8c

c) Alice decides to choose a new private key $a = 299$ with associated public key $A \equiv 2^{299} \equiv 34 \pmod{1373}$. Bob encrypts a message using Alice's public key and sends her the cipher text $(c_1, c_2) = (661, 1325)$. Decrypt the message

$m = (c_1^{a})^{-1} \cdot c_2 \pmod{p}$

$m \equiv ((661^{299})^{-1} \cdot 1325) \bmod 1373$

$m \equiv ((661^{229})^{-1} \bmod 1373)(1325 \bmod 1373) \bmod 1373$

$661^{229} \bmod 1373 = (920)$

$229 = 1 + 2 \cdot 114 = 1 + 2 \cdot 2 \cdot 57 = 1 + 4 + 2 \cdot 2 \cdot 2 \cdot 28 = 1 + 4 + 2 \cdot 2 \cdot 2 \cdot 2 \cdot 14$

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

$661^{299} \bmod 1373 = ((661^1)(661^4)(661^{32})(661^{64 \cdot 3})) \bmod 1373$

$(661^1)(661^4) = x$ let us say $\rightarrow$ $661 \cdot 885 \bmod 1373 = 87$

$= (x \bmod 1373)(661^{32} \cdot 661^{64 \cdot 3} \bmod 1373) \bmod 1373$

$= (x \bmod 1373)((661^{32} \bmod 1373)(661^{64 \cdot 3} \bmod 1373) \bmod 1373) \bmod 1373$

($661^{32} \bmod 1373 = 989$; $661^{64 \cdot 3} \bmod 1373 = 552$)

$661^3 \bmod 1373 = 1096$

2×6 mod 7 more times: $1214, 647, 297, 286, 789, 552$ (powers $2, 4, 8, 16, 32, 64$)

$(661^{2} \bmod 1373)^{2} \bmod 1373)^{2} \bmod 1373)^{2} \bmod 1373)^{2} \bmod 1373) \bmod 1373$

($661^2 \bmod 1373 = 307$; $307^2 \bmod 1373 = 885$; $885^2 \bmod 1373 = 615$; $615^2 \bmod 1373 = 650$; $650^2 \bmod 1373 = 989$)

$= (x \bmod 1373)(989 \cdot 552 \bmod 1373) \bmod 1373$

$= (x \bmod 1373)(847) \bmod 1373 = (87)(847) \bmod 1373 = 920$

$661^{229} \bmod 1373 = 920$

So what is $(661^{229})^{-1} \bmod 1373$? multiplicative inverse of $920 \pmod{1373}$

special case $a^{-1} \equiv a^{m-2}$ $a = 920$ $m = 1373$ if coprime

Case of Euler's theorem

2.8c
Continued

$a^{m-2} = 920^{1371}$ ~~Mod~~

$m = (920^{1371} \bmod 1373)(1325 \bmod 1373) \bmod 1373$

$1371 = 1 + 2 \cdot 685 = 1 + 2 + 2 \cdot 2 \cdot 342 = 1 + 2 + 2 \cdot 2 \cdot 2 \cdot 171 = 1 + 2 + 2^3 + 2^3 \cdot 170$

$= 1 + 2 + 2^3 + 2^4 \cdot 85 = 1 + 2 + 2^3 + 2^4 + 2^5 \cdot 42 = 1 + 2 + 2^3 + 2^4 + 2^6 \cdot 21 = 1 + 2 + 2^3 + 2^4 + 2^6 + 2^8 \cdot 10$

$= 1 + 2 + 2^3 + 2^4 + 2^6 + 2^8 \cdot 5 = 1 + 2 + 2^3 + 2^4 + 2^6 + 2^8 + 2^{10}$

$((920^1)(920^2)(920^{2^3})(920^{2^4})(920^{2^6})(920^{2^8})(920^{2^{10}})) \bmod 1373$

X = underlined 632 431 406 284 1004 1209

$(x \bmod 1373)(920^{2^6 \cdot 1209} \bmod 1373) \bmod 1373$

632 1254 431 406 76 284 1022 1004 234 1209
1 2 3 4 5 6 7 8 9 10

$920 \cdot 632 \bmod 1373$

$(661)(431) \bmod 1373 = 680$

$680 \cdot 406 \bmod 1373 = 107$

$107 \cdot 284 \bmod 1373 = 182$

$182 \cdot 1004 \bmod 1373 = 119$

$119 \cdot 1209 \bmod 1373 = \boxed{1079}$

$\Rightarrow (1079 \cdot 1325) \bmod 1373 =$

$\boxed{m = 382}$

Decrypted Message
382

2.17

A. $11^x = 21 \bmod 71$ (x = 37)
B. $156^x = 116 \bmod 593$ (x = 59)
C. $650^x = 2213 \bmod 3571$ (x = 319)

See attached code