Codebusters C - Solutions
UChicago 2019

Please don't redistribute.

Points awarded = max {0, min{*total, total - 100 · # of additional errors*}}
a.k.a. *(total - 100 · # of additional errors)* constrained to the range [0, total]
Time bonus is reduced to be more generous to slower teams.

Regional-level questions [Total of 3200 pts]

1. Timed Aristocrats w/ Hint [500 pts + Timing Bonus/4]:

Plaintext: `The missile knows where it is at all times. It knows this because it knows where it isn't, by subtracting where it is from where it isn't, or where it isn't from where it is, it obtains a difference, or deviation.`

Key ('a'->'p', 'b'->'h', ...):

```
a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z
p, h, g, m, v, q, u, r, s, a, t, o, e, z, w, y, b, d, l, j, k, x, c, n, i, f
```

2. Affine encryption [200 pts]:

Ciphertext: `Qllcxjck kmdpq kdyxjuwdexzy cg mgqn tud GGZ, JLG, ern hcjkucr.`

3. Affine encryption [200 pts]:

Ciphertext: `Vn ran roonaz, zd vn enno r gdl yrqgn yd fxgyjcgt`

4. Vigenère encryption [300 pts]:

Ciphertext: `Mssezozkfa ysepgflr fos opfobwfvie pbpbqfhbol wzac m zvajyuuuxf bqnofpjq zsoysf zcopsff.`

5. Vigenère decryption [300 pts]:

Plaintext: `I thought not. It's not a story the Jedi would tell you. It's a Sith legend.`

6. Spanish Caesar decryption [300 pts]:

Plaintext: `La mitocondria es la potencia de la célula (-> celula)`
Shift: 12

7. Baconian Cipher decryption [400 pts]:

Plaintext: `Steganographia`

8. Caesar cryptanalysis [500 pts]:
Plaintext: `All Gaul is divided into three parts, one of which the Belgae inhabit, the Aquitani another, and Gauls (known as Celts in their language) the third.`
Shift: 7

9. Mystery cryptanalysis [500 pts]: Aristocrats
Plaintext: Was James Bond actually a good spy if he was so famous and flashy?
Key ('a'->'j', 'b'->'h', ...):
```
a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z
j, h, r, c, a, x, d, g, y, z, n, e, t, m, s, k, u, v, o, f, p, w, b, q, l, i
```

State-level questions [Total of 1200 points]
These questions give fewer points than their difficulty to reduce the penalty of not being prepared for state level stuff.

10. RSA decryption [300 pts]:
Plaintext: `hello there`
p = 2, q = 13; e = d = 5, N = 26

11. Hill Cipher decryption [300 pts]:
Ciphertext: `gcj uwq yvi`
Plaintext: `fun scioly`
Column vectors: $[6,2,9]^T$, $[20, 22, 16]^T$, $[24, 21, 8]^T$
Decoded vectors (after being left-multiplied by the matrix):
$([57, 20, 13]^T \mod 26) = [5, 20, 13]^T$
$([148, 54, 60]^T \mod 26) = [18, 2, 8]^T$
$([144, 37, 50]^T \mod 26) = [14, 11, 24]^T$

12. Vigenère with crib cryptanalysis [300 pts]:
Plaintext: `Weather is sunny today but bring Alan Turing in case.`
Key: `enigma` (i.e., use the code "enigma" to get from the ciphertext to the plaintext)

13. Affine Cipher decryption [300 pts]:
Plaintext: `Have a gneiss and sodaliteful day!`
Key: a = -5, b = 15; $a^{-1} = 5$
D(y) $\equiv a^{-1}(y - b) \pmod{26}$
$\equiv a^{-1}y - a^{-1}b \pmod{26}$
Reasonable intermediary (after multiplying by $a^{-1}=5$ but before finding $a^{-1}b$): `Exsb x dkbfpp xka plaxifqbcri axv!` Give 150 points if they get this part correct.
And finding $a^{-1}b$ *(= 23)* is equivalent to breaking a Caesar cipher. But it seems reasonable when you can check that "`x`" corresponds to either "`a`" or "`I`".