Zac Foteff
Crypto

Project 5

(1) $\gcd(30030, 257)$

$30030 = 116(257) + 218$

$257 = 1(218) + 39$ $\gcd(30030, 257) = 1$

(2) Claim: 257 is prime

If 257 is composite, it must have a factor c such that $c < \sqrt{257}$

$\sqrt{257} = 16.031...$

Consider this definition applied to 30030

$\sqrt{30030} = 173.29$

We know the factors of 30030 includes 2, since the cannonical form of 30030 includes 2 and $2 \cdot 15015 = 30030$

Since we've proved in problem 1 that the $\gcd(30030, 257) = 1$ that means that 30030, 257 share no common factors. Additionally, we know that all numbers can be expressed in canonical form as a product of primes. Therefore, since 30030 and 257 share no common factors, and all numbers from 1 to 16 are included as part of the canonical form of 30030, that means that 257 must be prime

(3) Fermat's Little Theorum : $a^p \equiv a \mod p$

$$a^{p-1} \equiv 1 \mod p$$

Considering $2^{58} \mod 11$

$$2^{11-1} \equiv 1 \mod 11$$

$$2^{10} \equiv 1 \mod 11$$

$$1024 \equiv 1 \mod 11$$

$$\frac{1024-1}{11} = 93$$

(4) Affine encrypt $= (\alpha x + \beta) \mod 26$

$E(x, \beta)$ gives ciphertext c

$$E(x, \beta) = (\alpha x + \beta) \mod 26 \quad \text{where } \alpha \ \& \ 26 \text{ are coprime}$$

$$c = (\alpha x + \beta) \mod 26$$

$$c - \beta = \alpha x \mod 26$$

$$\alpha^{-1}(c-\beta) = \alpha^{-1}\alpha x \mod 26$$

$$\alpha^{-1}(c-\beta) = x \mod 26$$

$$\alpha^{-1}(c-\beta) \mod 26 = \text{Dec}(c, \beta)$$

(5) The Vignere Cipher is a poly alphabetic cipher that utilizes a Vignere table that contains 26 different permutations of the alphabet, and a key that is circularly generated until it matches the length of the plaintext message. So if the key is of length n, that means that the keyspace offers 26^n possibilities for a ciphertext

(6) 7^{803}. Everything should be mod 1000 for 3 digits

$\phi(1000) = \phi(2^3)\phi(5^3) = 2^3(1-\frac{1}{2}) \cdot 5^3(1-\frac{1}{5}) = 400$

using Euler we now know that

$7^{400} \equiv 1 \mod 1000$

$7^{803} = 7^{400} \cdot 7^{400} \cdot 7^3$

$7^3 = 343 \rightarrow$ last three digits

(7) $2^{43210} \mod 101$, Since 101 is prime we can use Fermat's little theorum

$2^{101-1} \equiv 1 \mod 101$

$2^{100} \equiv 1 \mod 101$

$\frac{2^{100}-1}{101} \mod 101 = 92$

8) Find $1835^{1910} + 1986^{2061} \equiv 0 \mod 7$

$1835 = (5 \cdot 367)^{2 \cdot 5 \cdot 191}$

by fermat: $5^6 \equiv 1 \mod 7$, $367^6 \equiv 1 \mod 7$

$(5^6)^{318} \equiv 1 \mod 7$, $(367^6)^{318} \equiv 1 \mod 7$

$5^{1908} \cdot 5^2 \equiv 1 \cdot 4 \mod 7$ $\quad 1 \cdot 4 \cdot 1 \cdot 2 = 8$

$367^{1908} \cdot 367^2 \equiv 1 \cdot 2 \mod 7$

$1835^{1910} = 8 \equiv 1 \mod 7$

$1986^{2061} = (2 \cdot 3 \cdot 331)^{3 \cdot 687}$

by fermat: $2^6 \equiv 1 \mod 7$, $3^6 \equiv 1 \mod 7$, $331^6 \equiv 1 \mod 7$

$(2^6)^{343} \equiv 1 \mod 7$, $(3^6)^{343} \equiv 1 \mod 7$, $(331^6)^{343}$

$2^{2058} \cdot 2^3 \equiv 1 \cdot 1 \mod 7$ $\quad 1 \cdot 6 \cdot 1 \cdot 1 \cdot 1 \cdot 1 = 6$

$3^{2058} \cdot 3^3 \equiv 1 \cdot 6 \mod 7$ $\quad 1986^{2061} = 6 \equiv 1 \mod 7$

$331^{2058} \cdot 331^3 \equiv 1 \cdot 1 \mod 7$ $\quad 6 + 8 \equiv 0 \mod 7$

9

$2^{1000} \bmod 77$

$\phi(77) = \phi(7) \cdot \phi(11) = 7\left(1-\frac{1}{7}\right) \cdot 11\left(1-\frac{1}{11}\right) = 60$

$2^{60} \equiv 1 \bmod 77$

$2^{1000} = 2^{60 \times 16} \cdot 2^{40} \bmod 77$

$2^{40} = \left(2^{10}\right)^{4} \bmod 77$

$2^{10} = 1024 \pmod{77}$

$= 23 \bmod 77$

$2^{1000} \bmod 77 = 23$

10

Let there be x number of people

$x \equiv 1 \mod 3$

$x \equiv 2 \mod 4$

$x \equiv 3 \mod 5$

use chinese remainder theorum

$p_1 = 3$, $p_2 = 4$, $p_3 = 5$, the system has a unique solution mod 60

$x = 20 \cdot (2 \cdot 1) + 15 \cdot (3 \cdot 2) + 12 \cdot (3 \cdot 3)$

$= 238$

$238 \mod 60 = 58$ is the smallest number of people

which means the next smallest number has to be $58 + 60 = 118$