Q1 35%
Q2 69%
Q3 82%
Q4 90%
Q5 80%
Q6 4%
Q7 90%
Q8 82%
Q9 70%
Q10 36%

Excellent (Q4 Q7)

E matrix (DES)
SBytes (AES)

Good (Q3, Q5, Q8)

IP^{-1}
S-boxes
Shift Rows

Average (Q2, Q9)

ADFGVX basics
AES key

Poor (Q1, Q6, Q10)

Hill Decrypt
DES key
AES mult

Modern Private Key / Symmetric $\Longrightarrow$ Public Key

$\hookrightarrow$ 1. Build up some math!!!

Number Theory
- Group Theory

EULER'S THEOREM

Fermat's Thm
if p is prime and $\gcd(a,p) = 1$,
Then $a^{p-1} \equiv 1 \pmod{p}$.

$$34^{66} \equiv 1 \pmod{67}.$$

modulo sys mod p a set of $p-1$ values
$a_1, a_2, \ldots a_{p-1}$ s.t. for any $i \neq j$ $1 \leq i < j \leq p-1$
$a_i \not\equiv a_j \pmod{p}$, and $a_i \not\equiv 0 \pmod{p}$ $a_j \not\equiv 0 \pmod{p}$

Consider $p=5$ $\{1,2,3,4\} \longmapsto$
$\{17,13,9,11\} \rightarrow \{2,3,4,1\}$
under mod

Start w/ the mod sys $S = \{1, 2, 3, \ldots, p-1\}$

Let a be s.t. $\gcd(a, p) = 1$

(Create a new set $S' = \{a, 2a, 3a, \ldots (p-1)a\}$
↳ each item is an item from the old set multiplied by a.

WANT TO PROVE S' is ALSO a mod sys mod p.

(1) all terms $\not\equiv 0 \pmod p$ since each is a product of 2 terms relatively prime to p.

(2) Prove that all items is S' are distinct mod p.

We use proof by contradiction.

Assume the opposite, that some 2 values are equivalent mod p. Namely $\exists\, i, j \in \mathbb{Z}$ $1 \le i < j \le p-1$ s.t. $ai \equiv aj \pmod p$

$ai - aj \equiv 0 \pmod p$

$a(i-j) \equiv 0 \pmod p$

$\Rightarrow p \mid (a(i-j))$

$\Rightarrow p \mid a$ or $p \mid (i-j)$

$p \mid a$ ✗ Given $\gcd(a, p) = 1$.

$p \mid (i-j)$ ✗ $i - j = 0$ because $|i-j| < p$ ↳ Contradicts i, j are unique.

Thus, our init assumption was incorrect.

It follows that all ~~elements~~ elements in S' are unique mod p

10/18/19 (4)

$S = \{1, 2, 3, \ldots p-1\}$

$S' = \{a, 2a, 3a, \ldots (p-1)a\}$

} both mod sys mod p

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} ai \pmod p$$

$$\left(\prod_{i=1}^{p-1} ai\right) - \prod_{i=1}^{p-1} i \equiv 0 \pmod p$$

$$a^{p-1}\left(\prod_{i=1}^{p-1} i\right) - \prod_{i=1}^{p-1} i \equiv 0 \pmod p$$

$$\left(\prod_{i=1}^{p-1} i\right)\left(a^{p-1} - 1\right) \equiv 0 \pmod p$$

$\Rightarrow$ either $p \mid \left(\prod_{i=1}^{p-1} i\right)$ OR $p \mid (a^{p-1} - 1)$ ✓✓

no item in product shares common factor with p.

$$a^{p-1} - 1 \equiv 0 \pmod p$$

$$\boxed{a^{p-1} \equiv 1 \pmod p}$$

$3^{100} \equiv 1 \bmod 101$ $\quad p = 101$ is prime

$3^{405} \equiv 3^{400} \times 3^5 \bmod 101$

$\equiv (3^{100})^4 \times 3^5 \bmod 101$

$\equiv 1^4 \times 3^5 \equiv \underline{243 \bmod 101} \equiv 41 \bmod 101$

What is remainder when 3^{405} divided by 101?

$\Downarrow$

(41)

Define $\phi(n)$ = the # of values in the Euler Phi Function set $\{1, 2, 3, \ldots, n\}$ that share no common factors with n.

$\phi(6) = 2$ ~~1 2 3 4 5 6~~

for an affine cipher w/ n symbols there are $\phi(n) * n$ possible keys.

$\phi(p) = p-1$ if $p \in$ Prime.

$\phi(p^k) = p^{k-1}(p-1)$

$= p^k - p^{k-1}$

$= p^k(1 - \frac{1}{p})$

25

				p columns
1	2	3	4	~~5~~
6	...			~~10~~
~~11~~				~~15~~
~~16~~				~~20~~
21				~~25~~

p^{k-1}

$p^{k-1}(p-1)$

If $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m) * \phi(n)$.

$\phi(p_1^{q_1} p_2^{q_2} p_3^{q_3} \cdots p_k^{q_k}) = (p_1^{q_1} - p_1^{q_1-1})(p_2^{q_2} - p_2^{q_2-1}) \cdots$

$= \prod_{i=1}^{k} p_i^{q_i} - p_i^{q_i-1} = \prod_{i=1}^{k} p_i^{q_i}(1 - \frac{1}{p_i})$

$= n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$

$\phi(2^3 \cdot 3^2 \cdot 5^1 \cdot 7^{10}) = (2^3 - 2^2)(3^2 - 3^1)(5^1 - 5^0)(7^{10} - 7^9)$

$= (2^3 \cdot 3^2 \cdot 5^1 \cdot 7^{10})(\frac{1}{2})(\frac{2}{3})(\frac{4}{5})(\frac{6}{7})$