Pseudoprimes

Wednesday, February 11, 2026 7:02 PM

Recall: FLT

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

1] Mersenne Primes:

a prime of this form $2^p - 1$ for a prime p.

e.g. let $p = 5$

$2^5 - 1 = 31$ is Mersenne prime

e.g. $2^{11} - 1 = 2047 = 23 \times 89$

Mersenne composite

2] Pseudoprime:

Let n be a composite and coprime to b.

if $b^{n-1} \equiv 1 \pmod{n}$, then n is pseudoprime to base b.

Note: for numbers $< 10^{10}$

455×10^6 primes

149×10^3 are pseudprimes to base 2.

if $2^{n-1} \equiv 1 \pmod{n}$

$$\text{Prop}(n \text{ is prime}) = \frac{455 \times 10^6}{455 \times 10^6 + 149 \times 10^3} \simeq 99.967\%$$

$$\text{Prop}(n \text{ is pseudoprime to base 2}) \cong 0.033\%$$

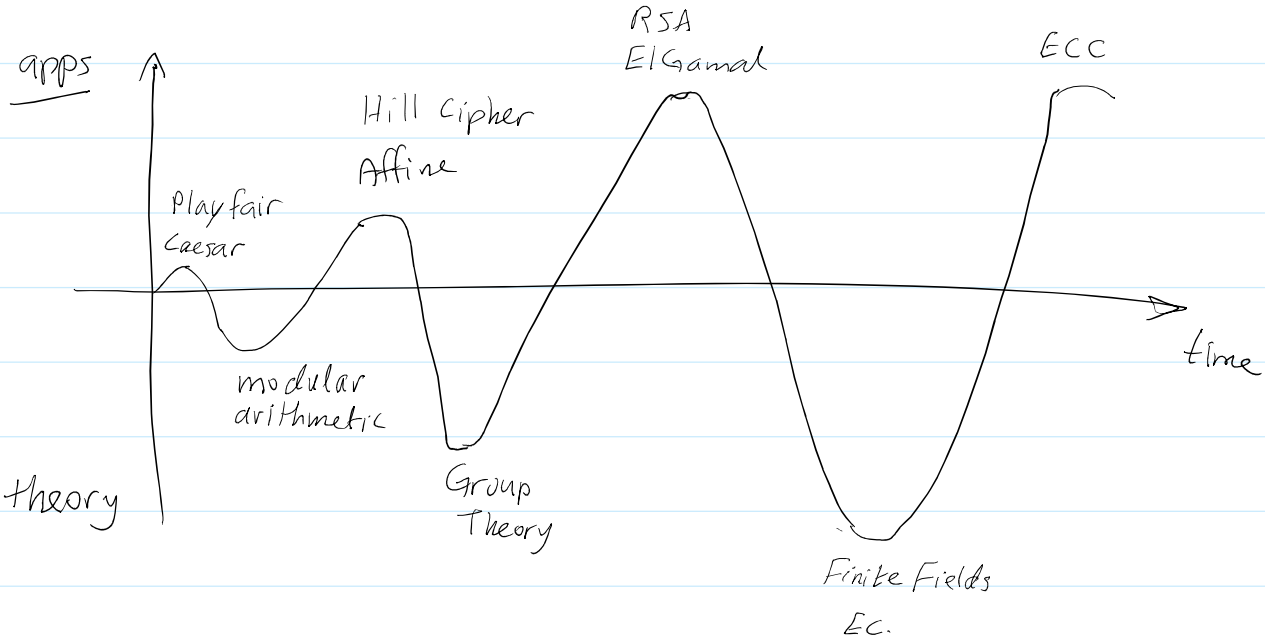
3] Def^n.

If n is composite and pseudoprime to all possible bases (coprime to n), then n is called a Carmichael number.

e.g. $561 = 3 \cdot 11 \cdot 17$ is Carmichael number.

$$7^{560} \equiv 1 \quad (561)$$

4] Map:



5] Affine scheme:

Plaintext: $a \rightarrow 2 \longrightarrow 0 - 25 \pmod{26}$

key $k = (a, b)$

Encryption:

$$E(p) = c = a \cdot p + b \pmod{26}$$

e.g. $p =$ ok

key $(a = 3,\ b = 2)$

P :	O	K
pVal :	14	10
	$3 \times 14 + 2$	$3 \times 10 + 2$
C val.	$44 \equiv 18$	$32 = 6$
C :	T	G

Decryption :

$$D(C) = (C - b) \cdot \tilde{a}^{1} \pmod{26}$$