Observations: $b^n - 1 = (b-1)(b^{n-1} + b^{n-2} + \cdots + 1)$

$b^{mn} - 1 = (b^m - 1)(b^{mn-m} + \cdots + 1)$

$x^n - 1 = (x-1)(x^{n-1} + \cdots + 1)$

$x^{mn} - 1 = (x^m - 1)(x^{m(n-1)} + x^{m(n-2)} + \cdots + 1)$

no roots of $x^{m(n-1)} + x^{m(n-2)} + \cdots + x^m + 1 = g(x)$ is an mth root of unity.

Q. Prove if $d = \gcd(m,n)$ & $a > 1$ an integer, then

$\gcd(a^m - 1, a^n - 1) = a^d - 1$.

Soln: set $m = dm_1$, $n = dn_2$

$a^m - 1 = (a^d - 1) f_{m_1}(a)$ & $a^n - 1 = (a^d - 1) f_{n_1}(a)$

$f_{m_i}(a) = a^{d(m_i - 1)} + a^{d(m_i - 2)} + \cdots + 1$ $\quad i = 1, 2$

$\gcd(f_{m_1}(a), f_{n_1}(a)) = 1$?

Observe $\gcd(f_{m_1}(x), f_{n_1}(x)) = 1$

Roots of $f_{m_1}(x)$ are $m = m_1 d$ roots of unity which not d roots of unity

" $f_{n_1}(x)$ are $n = n_1 d$ . . . . .

. . . . . .

$\Rightarrow$ $s f_{m_1}(a) + t f_{n_1}(a) = l$ for some $s, t \in \mathbb{Z}$ (e.g. when l is the gcd of $f_{m_1}(a)$ & $f_{m_2}(a)$.

↳ $s(x) f_{m_1}(x) + t(x) f_{n_1}(x) = 1$ for some $s(x) \& t(x) \in \mathbb{Z}[x]$

(initially they are in $\mathbb{Q}[x]$)

put $x = a$

$s(a) f_{m_1}(a) + t(a) f_{n_1}(a) = 1$

so that $f_{m_1}(a)$ & $f_{n_1}(a)$ are coprime.

Silver Pohlig - Hellman exponentiation ciphers.

Let p be <u>prime</u> & $e \in \mathbb{N}$ s.t. $0 < e < p$ &
$\gcd(e, p-1) = 1$ → called exponent.

[E.g., $p = 29$, $e = 3$, 5, or 9 ...]

$\Sigma : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ $\quad$ $m \longmapsto m^e$

$D : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ $\quad$ $m \longmapsto e^d$

so that $D\Sigma(m) = m$ $\quad$ $d = ?$

$\therefore (m^e)^d = m$

$\therefore \boxed{m^{de} = m}$

$\therefore \boxed{de \equiv 1 \mod p-1}$

since $\gcd(e, p-1) = 1$ $\exists$ s & t

s.t. $\boxed{se + t(p-1) = 1}$

so $se \equiv 1 \mod p-1$

$|U(\mathbb{Z}_p)| = p-1$

$m^{se} = m^{1 - t(p-1)}$
$= m \cdot (m^{p-1})^{-t}$
$= m \cdot 1^{-t}$
$= m$

Example Plain text HELLO

$A = \{A=0, \ldots, Z=25, !=26, .=27, ?=28\}$

$p = 29$ & chosen $e = 3$. $\quad$ $d = 19$ (so that $ed \equiv 1 \mod 28$)

$\mathcal{E}(H) = 7^3 = \underline{7 \times 20 \mod 29}$
$= 24 \mod 29$
$= Y$

$\mathcal{E}(E) = 4^3 = 6 \pmod{29}$
$= G$

$\mathcal{E}(L) = 11^3 = 11 \times 5 \mod 29$
$= 26 \mod 29$
$= !$

$\mathcal{E}(O) = 14^3 = 18 \pmod{29}$
$= S$

HELLO $\rightsquigarrow$ YG!!S

$\mathcal{D}(m) = \underline{m^{19} \mod 29}$

$\mathcal{D}(Y) = 24^{19} = 24 \times 5^{18} \mod 29$
$= 7 \mod 29$
$= H.$

Quadratic chipher.

$\mathcal{E}: \mathbb{Z}_n \to \mathbb{Z}_n$ $\quad m \mapsto m^2$ $\qquad \mathcal{D}: \mathbb{Z}_n \to \mathbb{Z}$?

$n = 26$

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a^2	0	1	4	9	16	25	10	23	12	3	22	17	6	7	14	17	22	3	12	23	10	1	16	25	18	9

$\mathbb{Z}_{26}$

COLOUR = 2-14-11-14-20-18 $\xrightarrow{\mathcal{E}}$ 4-14-17-14-10-12 = EOROKM

$\mathcal{D}(m) = \sqrt{m}$? $\qquad \mathcal{D}(10) = \{6, 20\}$, $\mathcal{D}(4) = \{2, 24\}$, $\mathcal{D}(14) = \{12, 14\}$

$\mathbb{Z}_2 = \{1, -1\}$ $\qquad \mathcal{D}(EOROKM)$ has 2^6 possibilities.

If only one make sure pick it & leave the rest.

RSA (Rivest - Shamir - Adleman) 1977

Here there are two type of keys ① public key ② private key

The private key is known to the receiver only.
The public key is in public domain.
After encryption the message is sent & anyone can see it.
The reciever can decrypt the message using the private key.
So these keys are generated by the reciever & the public key is announced.