Crypto 1 GÜ 10

Ex 32)

Wilson's primality criterion

$$\left\| \begin{array}{c} \text{If } n > 1 \text{ and prime} \\ \Leftrightarrow (n-1)! \equiv -1 \pmod n \end{array} \right\|$$

a.) $\boxed{\Rightarrow}$

If n is prime, $n>1$
$\Rightarrow (n-1)! \equiv -1 \pmod n$
holds

Let n and $n>1$ be prime each factor m of $(n-1)!$ is $\mathbb{Z}_n^*$ (multiplicative group)

$\Rightarrow$ Each factor m has an inverse in $\mathbb{Z}_n^*$

The $m=1$ and $m=p-1=-1$ are inverse to themselves, since:

$m \cdot m^{-1} = 1 \pmod n \Rightarrow m^2 \equiv 1 \pmod n$

$m = m^{-1}$

$\Rightarrow (m^2-1) = 0 \pmod n \Rightarrow (m+1)(m-1) \equiv 0 \pmod n$

$\Rightarrow m \in \{1, -1\}$

$$\Rightarrow (n-1)! \equiv \prod_{i=1}^{n-1} i = \underbrace{(n-1)}_{\text{self-inverse}} \cdot \underbrace{(n-2) \cdot \ldots \cdot 3 \cdot 2}_{\text{pairwise inverses}} \cdot \underbrace{1}_{\text{self-inverse}}$$

$\equiv (n-1) \equiv -1 \pmod n$

$\boxed{\Leftarrow}$

$(n-1)! \equiv -1 \pmod n$
holds only if n
is prime

Let $n = a \cdot b$ be composite,
$a, b \neq n$, a,b prime

$a | n$ and $a | (n-1)!$ // a divides one factor of $(n-1)!$

From $(n-1)! \equiv -1 \pmod n$ // use assumption

$\Rightarrow a \mid (n-1)! + 1 \Rightarrow a \mid 1$

$\Rightarrow a = 1 \Rightarrow n$ must be prime // contradiction

// (since $b \stackrel{!}{=} n$ prime)

$\square$

b.) 29 prime?

$$28! = \underbrace{(28 \cdot 27)}_{2} \underbrace{(26 \cdot 25)}_{12} \underbrace{(24 \cdot 23)}_{1} \underbrace{(22 \cdot 21)}_{27} \underbrace{(20 \cdot 19)}_{3}$$

mod 29 $\longrightarrow$

$$\cdot \underbrace{(18 \cdot 17)}_{16} \underbrace{(16 \cdot 15)}_{8} \cdot \underbrace{(14 \cdot 13)}_{8} \cdot \underbrace{(12 \cdot 11)}_{16} \cdot \underbrace{(10 \cdot 9 \cdot 8)}_{24}$$

$$\cdot \underbrace{(7 \cdot 6 \cdot 5 \cdot 4)}_{28} \underbrace{(3 \cdot 2)}_{6}$$

$= \dots$

$= -1 \pmod{29} \Rightarrow 29$ is prime

c.) No, since the calculation of the factorial is of high complexity. (comp.)

Ex 33.) The discrete logarithm

a.) group $\mathbb{Z}_{79}^*$, generator $a = 3$

compute $x = \log_3(18)$ with $x \in \mathbb{Z}_{79}^*$

(I) $3^x \equiv 18 \pmod{79} \Rightarrow$ exhaustive search

	$3^x \bmod 79$
$x = 0$	1
$x = 1$	3
$x = 2$	9
$x = 3$	27
$x = 4$	$81 \equiv 2$
$x = 5$	$243 \equiv 6$
$x = 6$	$729 \equiv 18$

$\Rightarrow \log_3(18) = 6$

Crypto 16410

$3^x = 1 \pmod{\cancel{7}9}$

From Euler-Fermat we know that:

$a^{p-1} = 1 \pmod p \Rightarrow x = p-1 = \underline{\underline{78}}$

b.) The worst case would be 78 trials
$\Rightarrow$ multiplication of large numbers is comp. complex
$\Rightarrow$ no efficient algorithm for the calculation of the discr. log is known

Ex 34) primitive elements (PE)

$\boxed{\text{"}\Rightarrow\text{"}}$ If a is a PE mod p $\Rightarrow \mathrm{ord}_p(a) = p-1$ // by def.

$\Rightarrow \forall i : a^{\frac{p-1}{p_i}} \not\equiv \underline{1} \pmod p$

$\boxed{\text{"}\Leftarrow\text{"}}$ If a is not a PE (mod p),

~~ord_p~~ $\mathrm{ord}_p(a) = k$ and $k \mid (p-1)$

$\Rightarrow \exists c \neq 1$ with $p-1 = k \cdot c$, since $c \neq 1$, it holds

- $p_i \mid c$ for some i:

For that i, we get $a^{\frac{p-1}{p_i}} \equiv a^{\frac{k \cdot c}{p_i}}$

$\equiv (\underbrace{a^k}_{\equiv 1})^{\frac{c}{p_i}} \equiv 1 \pmod p$ $\square$

Ex 35.) Diffie-Hellman key exchange

$p = 107, \quad a = 2 \quad x_A = 66 \quad x_B = 33$

a.) A sends $\rightarrow B$: $n \equiv a^{x_A} \pmod p \equiv 2^{66} \pmod{107}$

$\equiv (2^{10})^6 \cdot 2^6 \equiv (61 \cdot 2)^6 \equiv 15^6$

$\equiv 11390625 = 47 \pmod{107}$

B → A: $\quad v = a^{x_B} \pmod{p}$

$= 2^{33} \pmod{107} = (61 \cdot 2)^3 = \dots$

$= \underline{\underline{58}} \pmod{107}$

A computes the shared key: $v^{x_A} \pmod{p}$

$[66_{10} = 1000010_2] \quad \longleftrightarrow \quad = 58^{66} \pmod{107}$

$\Rightarrow \quad 58^{66} \pmod{107} = ((((((58^1)^2 \cdot \underbrace{\cancel{58^0}}_{1})^2 \cdot \underbrace{\cancel{58^0}}_{1})^2 \cdot \underbrace{\cancel{58^0}}_{1})^2 \cdot \underbrace{\cancel{58^0}}_{1})^2 \cdot 58^1)^2 \cdot \underbrace{\cancel{58^0}}_{1}$

	58	(mod 107)
square → s	3364	47
s	2209	69
s	4761	53
s	2809	27
s	729	37
multiply M	5046	17
s	289	$\underline{\underline{75}}$

B computes the shared key $u^{x_B} \pmod{p} = 47^{33} \pmod{107}$

<u>S & M</u> $\quad 33_{10} = 100001_2$

	47	(mod 107)
s	2209	69
s	4761	53
s	2809	27
s	729	87
s	7564	79
M	3713	$\underline{\underline{75}}$

⇒ 75 is the shared key of A and B