Tutorial 10

P2) $n = p \cdot q$, $p \neq q$ primes, $x^2 \equiv 1 \pmod n$, $x \not\equiv \pm 1 \pmod n$

Then $gcd(x+1, n) \in \{p, q\}$

$[x^2 \equiv 1 \pmod n \;\wedge\; x \not\equiv \pm 1 \pmod n] \Rightarrow 2 \leq x \leq n-2$

$x^2 \equiv 1 \pmod n \Leftrightarrow (x-1)(x+1) \equiv 0 \pmod n$

$\Leftrightarrow (x+1)(x-1) = k \cdot p \cdot q \quad \exists k \in \mathbb{N}$

Due to $x-1 < x+1 \leq n-1 < n = p \cdot q$

Hence, neither $x-1$ nor $x+1$ can divide both numbers p and q jointly.

$\Rightarrow gcd(x+1, n) \in \{p, q\}$

P3 (a) If m is not coprime to n, then $p \mid m$ or $q \mid m$ ↑ $p \neq q$

Hence, $gcd(m,n) \in \{p, q\}$ can be easily calculated.

We may easily calculate the private key, because we may assess $\phi(n) = (p-1)(q-1)$ because p and q are known and applying EEA on $gcd(e, \phi(n))$ reveals d. ✓

b) m, n have common divisors

The number of relatively prime numbers to n

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1$$

$$P(gcd(m,n) \neq 1) = 1 - \frac{\phi(n)}{n-1} = \frac{n-1-\phi(n)}{n-1}$$

$$= \frac{p \cdot q - 1 - p \cdot q + p + q - 1}{p \cdot q - 1} = \frac{p+q-2}{p \cdot q - 1} = \underline{P}$$

c) n : 1024 bits, $p \approx \sqrt{n} \approx 2^{512}$; $q \approx \sqrt{n} \approx 2^{512}$

$$\underline{P} = \frac{2^{512} + 2^{512} - 2}{2^{512} \cdot 2^{512} - 1} \approx 2^{-511} \approx (2^{-10})^{51} \cdot 2^{-1} \approx (10^{-3})^{51} \cdot 2^{-1}$$

$$= 5 \cdot 10^{-154}$$

P3/ Shamir's no key protocol: $p = 31337$, $a = 9999$, $b = 1011$
$m = 3567$.

a) $c_1 = m^a \bmod p = 3567^{9999} \bmod 31337 = 6399$

$c_2 = c_1^b \bmod p = 6399^{1011} \bmod 31337 = 29872$ (Hint)

$c_3 = c_2^{a^{-1}} \bmod p = 29872^{14767} \bmod 31337 = 24982$

$[\, m = c_4 = c_3^{b^{-1}} \bmod p = 3567 \,]$

$9999 = (\ldots)_2$

Bit	S	M
1	3567	X
0	667	—
0	6171	—
1	6786	13498
1	2686	23177
1	25812	3298
0	2865	
0	29268	
0	18929	
0	31120	
1	15752	143
1	20449	20384
1	10173	30182
1	17871	6399

We need to compute a^{-1} modulo $p-1$, we use the EEA

$gcd(c,d) = gcd(31336, 9999)$ $\quad c = p-1,\ d = a$

a_n	b_n	f_n	r_n	c_n	d_n
			$a = 31336$	1	0
			$d = 9999$	0	1
31336	9999	3	1339	1	-3
9999	1339	7	626	-7	22
1339	626	2	87	15	-47
626	87	7	17	-112	351
87	17	5	2	575	-1802
17	2	8	**1**	-4712	14767

$\Rightarrow gcd(31336, 9999) = 1 = -4712 \cdot 31336 + 14767 \cdot 9999$

$a_n = f_n \cdot b_n + r_n \qquad r_n < b_n$

$r_n = c_n \cdot c + d_n \cdot d$

$c_n = c_{n-2} - f_n \cdot c_{n-1}$

$d_n = d_{n-2} - f_n \cdot c_{n-1}$

Goal: $gcd(c,d) = e \cdot c + f \cdot d \qquad e, f \in \mathbb{Z}$