MATH 75: Cryptography **Spring 2022**

PSET 7 — May 24, 2022

Prof. Asher Auel ***Student: Amittai Siavava***

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***The Code Book*** by **Simon Singh**.
(b) ***Cryptography*** by **Simon Rubinsen-Salzedo**

Problems

1. For the following integers either provide a witness for the compositeness of n or conclude that n is probably prime by providing 5 numbers that are not witnesses. Recall that a witness for the compositeness of n is an integer $a \in \mathbb{Z}$ such that, if we write $n-1 = 2^k u$, where u is odd, then a satisfies $a \not\equiv 0 \pmod{n}$ and $a^u \not\equiv 1 \pmod{n}$ and $a^{2^i u} \not\equiv -1 \pmod{n}$ for all $i = 1, \ldots, k-1$.

(a) $n = 1009$.

$$\begin{aligned}
2^{1008} &\equiv 1 \pmod{1009} \\
3^{1008} &\equiv 1 \pmod{1009} \\
5^{1008} &\equiv 1 \pmod{1009} \\
7^{1008} &\equiv 1 \pmod{1009} \\
11^{1008} &\equiv 1 \pmod{1009} \\
13^{1008} &\equiv 1 \pmod{1009} \\
17^{1008} &\equiv 1 \pmod{1009}
\end{aligned}$$

Thus, 1009 is probably prime.
(It actually is! I computedthe values all the way to $1008^{1008} \pmod{1009}$ and they are all equivalent to 1)

(b) $n = 2009$.

$$\begin{aligned}
2^{2008} &\equiv 1773 \pmod{2009} \\
3^{2008} &\equiv 1313 \pmod{2009} \\
5^{2008} &\equiv 1535 \pmod{2009} \\
7^{2008} &\equiv 980 \pmod{2009} \\
11^{2008} &\equiv 221 \pmod{2009} \\
13^{2008} &\equiv 1240 \pmod{2009} \\
17^{2008} &\equiv 1082 \pmod{2009}
\end{aligned}$$

Thus, 2009 is NOT prime.

2. Using big-O notation, estimate the number of bit operations required to perform the witness test on $n \in \mathbb{Z}_{>0}$ enough times so that, if n passes all of the tests, it has less than a 10^{-m} chance of being composite.

3. Factor 53477 using the Pollard rho algorithm.

Running pollard's rho algorithm on 53477:

iteration	x	y	$\gcd(\|x-y\|, n)$
1	5	26	1
2	26	30514	1
3	677	15172	1
4	30514	6215	1
5	16150	5526	1
6	15172	4837	53

Thus, two non-trivial factors of 53477 are 53 and $\frac{53477}{53} = 1009$.

4. Fermat and sieving.

(a) Find three nontrivial factors of $n = 99999999999999999999999999999999999919$ by hand.

We know that every odd composite is a difference of squares. Let's find these two squares.
Starting at $a_0 = \lceil \sqrt{n} \rceil = 10000000000000000000$

$$\begin{aligned} 99999999999999999999999999999999999919 &\mod 10000000000000000000 = 9999999999999999919 \\ 99999999999999999999999999999999999919 &\mod 10000000000000000001 = 9999999999999999921 \\ 99999999999999999999999999999999999919 &\mod 10000000000000000004 = 9999999999999999939 \\ 99999999999999999999999999999999999919 &\mod 10000000000000000009 = 0 \end{aligned}$$

Thus, we see that 10000000000000000009 is a factor,
as is $\frac{99999999999999999999999999999999999919}{10000000000000000009} = 9999999999999999991$.
Further iteration doesn't yield interesting factors. However, we have not checked for small factors!
When we check small integers for factors, we see that
$23 \cdot 43478260869565217391304347826086953 = 99999999999999999999999999999999999919$

Thus, $\{23, 10000000000000000009, 9999999999999999991, 43478260869565217391304347826086953\}$
are factors of n.

(b) Let $n = 2^{29} - 1$. Given that

$$\begin{aligned} 258883717^2 &\equiv -2 \cdot 3 \cdot 5 \cdot 29^2 \pmod{n} \\ 301036180^2 &\equiv -3 \cdot 5 \cdot 11 \cdot 79 \pmod{n} \\ 126641959^2 &\equiv 2 \cdot 3^2 \cdot 11 \cdot 79 \pmod{n} \end{aligned}$$

discover a factor of n.

$$\begin{aligned} 258883717^2 &\equiv -2 \cdot 3 \cdot 5 \cdot 29^2 \pmod{n} \\ 301036180^2 &\equiv -3 \cdot 5 \cdot 11 \cdot 79 \pmod{n} \\ 126641959^2 &\equiv 2 \cdot 3^2 \cdot 11 \cdot 79 \pmod{n} \\ 258883717^2 \cdot 301036180^2 \cdot 126641959^2 &\equiv 2^2 \cdot 3^4 \cdot 11^2 \cdot 29^2 \cdot 79^2 \pmod{n} \\ (258883717 \cdot 301036180 \cdot 126641959)^2 &\equiv (2 \cdot 3^2 \cdot 11 \cdot 29 \cdot 79)^2 \pmod{n} \end{aligned}$$

$a^2 \equiv b^2 \pmod{n}$ implies that $n \mid (a+b)(a-b)$ (since $a^2 - b^2 \equiv 0 \pmod{n}$).
If n does not divide one of the two factors, then $\gcd(a-b, n)$ is a factor of n.
More precisely, $\gcd(a-b, n) \cdot \gcd(a+b, n) = n$

$$\begin{aligned} a &= 258883717 \cdot 301036180 \cdot 126641959 = 9869634044174622775396540 \\ b &= 2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 29 \cdot 79 = 2268090 \end{aligned}$$

$$\begin{aligned} \gcd(a-b, n) &= 1103 \\ \gcd(a+b, n) &= 486737 \\ 1100 \cdot 486737 &= n \end{aligned}$$

Thus, $a_1 = 1103$ and $a_2 = 486737$ are factors of n.

5. Discrete logarithms.

(a) Let $p = 101$. Compute $\log_2 11$ (using complete enumeration by hand).

$$2^{-1} \pmod{101} = 51$$

$$11 \tag{1}$$

$$\Downarrow$$

$$\frac{11}{2} \equiv 11 \cdot 51 = 561 \equiv 56 \pmod{101} \tag{2}$$

$$\frac{56}{2} = 28 \pmod{101} \tag{3}$$

$$\frac{28}{2} = 14 \pmod{101} \tag{4}$$

$$\frac{14}{2} = 7 \pmod{101} \tag{5}$$

$$\frac{7}{2} \equiv 7 \cdot 51 = 357 \equiv 54 \pmod{101} \tag{6}$$

$$\frac{54}{2} = 27 \pmod{101} \tag{7}$$

$$\frac{27}{2} \equiv 27 \cdot 51 = 1377 \equiv 64 \pmod{101} \tag{8}$$

$$\frac{64}{2} = 32 \pmod{101} \tag{9}$$

$$\frac{32}{2} = 16 \pmod{101} \tag{10}$$

$$\frac{16}{2} = 8 \pmod{101} \tag{11}$$

$$\frac{8}{2} = 4 \pmod{101} \tag{12}$$

$$\frac{4}{2} = 2 \pmod{101} \tag{13}$$

Thus, $\log_2 11 = 561 \pmod{101}$.

(b) Let $p = 27781703927$ and $g = 5$. Suppose Alice and Bob engage in a Diffie-Hellman key exchange; Alice chooses the secret key $a = 1002883876$ and Bob chooses $b = 21790753397$. Describe the key exchange: what do Alice and Bob exchange, and what is their common (secret) key? *[You may want to use a computer!]*

Alice sends Bob $a^* = g^a \pmod{p} \equiv 5281680355$.
Bob sends Alice $b^* = g^b \pmod{p} \equiv 22361055346$.
Their shared key is $g^{ab} \pmod{p} \equiv 17849372203$.
Alice computes $g^{ab} = (b^*)^a \pmod{p}$.
Bob computes $g^{ab} = (a^*)^b \pmod{p}$.
Thus, they can both find their shared key, and share information, without either knowihng the other's secret key.

(c) Let $p = 1021$. Compute $\log_{10} 228$ using the baby step-giant step algorithm. Show the output of, and explain all steps in, your computation.

$$\begin{aligned} p &= 1021 \\ h &= 228 \\ g &= 10 \\ m = \lceil \sqrt{p} \rceil &= 32 \end{aligned}$$

babysteps $= [h, hg, hg^2, hg^3, \ldots, hg^{m-1}]$
giantsteps $= [g^m, g^{2m}, g^{3m}, \ldots, g^{m^2}]$
Common: $hg^{31} \equiv 921 \equiv g^{16m} \pmod{1021}$

Thus:

$$\begin{aligned} hg^{31} &= g^{16m} \\ h &= \frac{g^{16m}}{g^{31}} = g^{16m-31} \\ \log h &= (16m - 31) \cdot \log g \\ \log_g h &= 16m - 31 \end{aligned}$$

Thus, $\log_{10} 228 \pmod{1021} = 16 \cdot 32 - 31 = 481$ Which we can confirm by computing $10^{481} \pmod{1021}$, which is (and should be) equivalent to 228

(d) Let $p = 1801$. Compute $\log_{11} 249$ using the Pohlig–Hellman algorithm. Show the output of, and explain all steps in, your computation. You'll want to remind yourself of how to solve systems of congruence equations using Sunzi's theorem: To find $x \in \mathbb{Z}$ satisfying $x \equiv a_i \pmod{n_i}$ for $i = 1, \ldots, k$, first define integers $N_i = \prod_{j \neq i} n_i$ and $M_i \equiv N_i^{-1} \pmod{n_i}$ for all $i = 1, \ldots, k$, and then $x = \sum_{i=1}^{k} a_i N_i M_i$ works.

Let $x = \log_{11} 249 \pmod{1801}$.
Then, $11^x \equiv 249 \pmod{1801}$.

$$\begin{aligned}
p &= 1801 \text{ (This is a prime number)} \\
\phi(p) = p - 1 &= 1800 \\
\phi(p) &= 2^3 \cdot 3^2 \cdot 5^2 \\
a &= \{7, 7, 6\} \\
N &= \{\ 3^2 \cdot 5^2, 2^3 \cdot 5^2, 2^3 \cdot 3^2\} = \{225, 200, 72\} \\
M &= \{1, 5, 8\} \\
x &= \sum_{i=1}^{k} a_i N_i M_i \\
x &= 7 \cdot 225 + 7 \cdot 200 \cdot 5 + 6 \cdot 72 \cdot 8 \\
x &= 12031 \\
x &\equiv 1231 \pmod{1800}
\end{aligned}$$

Thus, $\log_{11} 249 \pmod{1801} = 1231$.