Homework Answer Math 116

Jerry Liu, 404474229
Department of Mathematics
Date: February 11, 2016
University of California, Los Angeles

Homework Problems

Problem 1.

Solution. We know $n = 11413$ and $e = 7467$. We also know $n = 101 \cdot 113$.
$\phi(n) = (101-1)\cdot(113-1) = 11200$
$ed \equiv 1\ (mod\ \phi(n)) \Rightarrow\ \exists\, d, y \in \mathbb{Z}$ such that $ed + ny = 1$
By runing extended Euclidean Algorithm, we get:
$d \equiv 3$ (mod n)
Plaintext: $c^3 \equiv 5859^3 \equiv m \equiv 1415 \pmod{n}$

Problem 4.

Solution. Since 101 is a prime, by Fermat's Little Theorem, $a^{100} \equiv 1 \pmod{101}$.
Want to find: $3d \equiv 1 \pmod{100}$
By using extended Euclidean Theorem, we get: $d = 67$.
So, to decrypt: $m \equiv c^{67} \pmod{101}$

Problem 7.

Solution. We know modulus is n and public key exponent is e.
Let $c_{eve} = 2^e c \pmod{n}$, and private key be d
Nelson decrypts c_{eve}:

$$\begin{aligned} m_{eve} &\equiv c_{eve}^d \equiv (2^e c)^d \\ &\equiv 2^{ed} c^d \equiv 2m \pmod{n} \end{aligned}$$

Now Eve only needs to divide m_{eve} by 2 to get m since $\gcd(2, n) = 1$.

Problem 8.

Answer. The double encryption does not increase security.
It is the same as a single encryption with exponent $e = e_1 e_2$.

Problem 9.

p, q primes, $n = pq$ and $\gcd(x, pq) = 1$.

Part a.

Proof. By Euler's Theorem, $x^{\phi(n)} \equiv 1 \pmod{\phi(n)}$ and $\phi(n) = (p-1)(q-1)$
$x^{\frac{\phi(n)}{2}} \equiv x^{\frac{(p-1)(q-1)}{2}} \equiv (x^{p-1})^{\frac{k}{2}} \pmod{n}$, where $k = q-1$
And by Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow (x^{p-1})^{\frac{k}{2}} \equiv 1^{\frac{k}{2}} \equiv 1 \pmod{p}$.
Similarly, $x^{\frac{\phi(n)}{2}} \equiv 1 \pmod{q}$ □

Part b.

Proof. $x^{\frac{\phi(n)}{2}} \equiv 1$ both $\mod p$ and $\mod q \Leftrightarrow (x^{\frac{\phi(n)}{2}} - 1)$ is a multiple of both p and q
By the Lemma to Chinese Remainder Theorem, $x^{\frac{\phi(n)}{2}} - 1$ is a multiple of $n = pq$
$\Rightarrow x^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n}$ □

Part c.

Proof. Since $ed \equiv 1 \pmod{\frac{1}{2}\phi(n)}$, then $\exists\, y \in \mathbb{Z}$ such that $ed + \frac{1}{2}\phi(n)y = 1$
Then

$$ed = 1 - \frac{1}{2}\phi(n)y$$

$$\Rightarrow x^{ed} \equiv x^{1-\frac{1}{2}\phi(n)y} \equiv x \cdot x^{-\frac{1}{2}\phi(n)y} \equiv x \cdot (x^{\phi(n)})^{-\frac{1}{2}y} \equiv x \cdot 1 \equiv x \pmod{n}$$

□

Problem 10.

Answer. $e = 1$ means no encryption; since $(p-1)$ and $(q-1)$ are even numbers, $e = 2$ means $\gcd(e, (p-1)(q-1)) \neq 1$, which is not allowed in RSA.

Problem 12.

Solution. We know

$$516107^2 \equiv 7 \pmod{n}$$
$$187722^2 \equiv 2^2 \cdot 7 \pmod{n}$$

$\Rightarrow 187722^2 \equiv 2^2 \cdot 516107^2 \pmod{n}$
$\Rightarrow 187722^2 \equiv 1032214^2 \pmod{n}$. Since $1032214 \not\equiv 187722 \pmod{n}$,
we have two non-trivial factors:

$$p, q = \gcd(1032214 + 187722, n), \gcd(1032214 - 187722, n) = 569, 1129$$

Problem 14.

Solution. Since $x^2 \equiv 49 \pmod{pq}$, and $x \not\equiv \pm 7 \pmod{pq}$, we can use Chinese Remainder Theorem to find:

$$\begin{aligned} x &\equiv 7 \pmod{p}, \qquad x \equiv -7 \pmod{q} \\ \Rightarrow x^2 &\equiv 49 \pmod{p}, \qquad x^2 \equiv 49 \pmod{q} \\ \Rightarrow x^2 &\equiv 49 \pmod{pq} \end{aligned}$$

Problem 16.

Solution. Since e_A, e_B are relatively prime, $\exists\, x, y \in \mathbb{Z}$ such that $e_A x + e_B y = 1$. Eve can do the following:

1. Use extended Euclidean Algorithm to find such x, y
2. $c_{Eve} \equiv c_A^x \cdot c_B^y \equiv m^{e_A x + e_B y} \equiv m^1 \equiv m \pmod{n}$

Problem 19.

Part a.

Proof. Assume $\gcd(a, n) = 1$, let $m = \phi(n) \cdot k = k(p-1)(q-1)$ for some $k \in \mathbb{Z}$.
By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$.

$$a^m \equiv a^{k(q-1)(p-1)} \equiv (a^{p-1})^{k(q-1)} \equiv 1^{k(q-1)} \equiv 1 \pmod{p}$$

Similarly,

$$a^m \equiv 1 \pmod{q}$$

□

Part b.

Proof. If $\gcd(a, n) = 1$, $a^{m+1} \equiv a^m \cdot a \equiv 1 \cdot a \equiv 1$, both $\bmod p$ and $\bmod q$.
Otherwise, $\gcd(a, n) \neq 1$, $\Rightarrow \gcd(a, n) = p$ or $q \Leftrightarrow a \equiv 0 \bmod p$ or $\bmod q$.
Assume $a \equiv 0 \pmod{p}$, then $0^{m+1} \equiv 0 \pmod{p}$.
$\Rightarrow a^{m+1} \equiv a \pmod{p} \qquad \forall\, a \in \mathbb{Z}$.
Similarly,
$\Rightarrow a^{m+1} \equiv a \pmod{q} \qquad \forall\, a \in \mathbb{Z}$. □

Part c.

Proof. Since $ed \equiv 1 \pmod{\phi}(n) \Leftrightarrow ed - 1 = \phi(n) \cdot k$ for some $k \in \mathbb{Z}$.
By Euler's Theorem,
if $\gcd(a, n) = 1$, $a^{\phi(n)} \equiv 1 \pmod{n} \Rightarrow a^{k\phi(n)} \equiv (a^{\phi(n)})^k \equiv 1^k \equiv 1 \pmod{n}$
Let m in Part b be $ed - 1$, by Part b we know $a^{ed} \equiv a^{m+1} \equiv a \pmod{n} \quad \forall\, a \in \mathbb{Z}$ □

Part d.

Since $\mathbf{P}[\gcd(a, n) \neq 1] = \frac{1}{p} \cdot \frac{1}{q}$, when p and q are large, the probability becomes really small.
$\Rightarrow \mathbf{P}[\gcd(a, n) = 1] = 1 - \mathbf{P}[\gcd(a, n) \neq 1]$ becomes large
$\Rightarrow$ it is likely that $\gcd(a, n) = 1$ for a random a.

Problem 23.

Solution. Since $\gcd(12345, e) = 1$, $\exists\, x, y \in \mathbb{Z}$ such that $12345x + ey = 1$.
Therefore, to decrypt the cipher, we first find such x, y, and then:

$$(1^{12345})^x c^y \equiv m^{12345x} (m^e)^y \equiv m^{12345x + ey} \equiv m^1 \equiv m \pmod{n}$$

Computer Problems

Problem 2.

Solution. Odd number m and power k: $m, k = 58584121864443279685, 5$
Factors: $p, q = 740876531, 969862097$

Problem 6.

Solution. Factors: $p, q = 54378659, 9876469$

Problem 8.

Part a.

Solution. Factors: $p, q = 12347, 54323$

Part b.

Solution. Factors: $p, q = 670726081, 1$
This one doesn't help, since $a + b = n$ and $a - b$ is *coprime* to n.
Therefore it reveals nothing about the factorization.

Problem 14.

Part a.

Proof. By definition of RSA, $\forall\, m \in \mathbf{M} = \{0, 1, 2 \dots n_i - 1\}$

$$\Rightarrow 0 \leq m < n_i.$$
$$\Rightarrow 0 \leq m^3 < n_1 n_2 n_3.$$

□

Part b.

Proof. Since n_1, n_2, n_3 are coprimes to each other, by *Chinese Remainder Theorem*, we can calculate in this way:

1. For $i = 1, 2, 3$, let $z_i =$ product of n_1, n_2, n_3 except n_i
2. For $i = 1, 2, 3$, let $y_i = z_i^{-1} \pmod{n}$
3. Let

$$\begin{aligned} x &= m^3 y_1 z_1 + m^3 y_2 z_2 + m^3 y_3 z_3 \pmod{n_1 n_2 n_3} \\ &= m^3 \pmod{n_1 n_2 n_3} \end{aligned}$$

$x \equiv m^3 \pmod{n_i}$ and $0 \leq m^3 < n_1 n_2 n_3 \Rightarrow x = m^3$
m is coprime to $n_1 n_2 n_3$. $\Rightarrow$ we just need to take $\sqrt[3]{x}$ to get the actual m □

Part c.

Solution. Using Generalized Chinese Remainder Theorem

Corresponding y_i's and z_i's:
Using Python functions to calculate inverses

$$(y_1, z_1) = (216851051457, 493842074127513750694557613)$$
$$(y_2, z_2) = (2933660999772, 109743786018234293085678823)$$
$$(y_3, z_3) = (28806927150227, 27437049443922098827902019)$$

$$\sum_{i=1}^{3} c_i y_i z_i \pmod{n} = 52189581153668510460961337 5$$

Answer. 805121215

Note. The output is 805121214.9999999 since floating point is not accurate.

Source Code

`https://github.com/jerrylzy/Math116`

Project

Main Idea: I want talk about the weaknesses of WEP and the improvement of WP2 encryption.
WEP, as insecure as it is, is still used in some places, including public hotspot and home routers.
It is really weak and almost protects nothing from the user who broadcasts information to anyone around him/her.
Then I want to talk about how WPA/WPA2 solves problems of WEP and what challenges WPA/WPA2 faces.

Reference:

Security Improvement of WPA 2:
Nazmus Sakib, Fariha Tasmin Jaigirdar,
Muntasim Munim, Armin Akter,
Chittagong University of Engineering & Technology,
Chittagong, Bangladesh, Vol. 3 No.1, 2011.

What?s Wrong With WEP?
InteropNet Labs, 2011.

Intercepting Mobile Communications: The Insecurity of 802.11:
Nikita Borisov, Ian Goldberg, David Wagner
University of California, Berkeley, 2001.