EMAT10001 Workshop Sheet 6.

Conor Houghton 2013-11-2

Introduction

There is the usual bounty for errors and typos, 20p to £2 depending on how serious it is.

Some of these questions are taken from *Number Theory with Computer Applications* by Ramanujachary Kumanduri and Cristina Romero.

Useful facts

- Fermat's Little Theorem. Let p be a prime. Then $a^p \equiv a \pmod{p}$. In particular, if $p \not| a$ then $a^{p-1} \equiv 1 \pmod{p}$.
- Euler's Theorem. If a and m are integers such that $(a, m) = 1$ then

$$a^{\phi(m)} \equiv 1 \pmod{m} \tag{1}$$

- Pohlig-Hellman exponentiation cipher. Let p be a prime and e an integer such that $0 < e < p - 1$ and $(e, p - 1) = 1$, these are the secret key. If m_i is a text block with $0 < m_i < p$ then

$$c(m_i) \equiv m_i^e \pmod{p} \tag{2}$$

  is the encoded message and

$$[c(m_i)]^d \equiv m_i \pmod{p} \tag{3}$$

  returns the original message where $d \equiv e^{-1} \pmod{p-1}$.
- RSA public key cipher. Let m be an integer with $n = pq$ and p and q primes, let $0 < e < \phi(n) = (p-1)(q-1)$ be an integer such that $(e, \phi(n) = 1$. n and e are the public keys, p, or equivalently q or equivalently $\phi(n)$ is the private key. If m_i is a text block with $0 < m_i < n$ then

$$c(m_i) \equiv m_i^e \pmod{n} \tag{4}$$

  is the encoded message and

$$[c(m_i)]^d \equiv m_i \pmod{n} \tag{5}$$

  returns the original message where $d \equiv e^{-1} \pmod{\phi(n)}$.
- Handy alphabet chart

a	0	b	1	c	2	d	3	e	4	f	5	g	6	h	7
i	8	j	9	k	10	l	11	m	12	n	13	o	14	p	15
q	16	r	17	s	18	t	19	u	20	v	21	w	22	x	23
y	24	z	25												

- If $n = \prod p_i^{r_i}$ for primes p_i and integers r_i then

$$\phi(n) = n \prod \left(1 - \frac{1}{p_i}\right) \tag{6}$$

Some common mathematical notation

- The Greek alphabet (little, capital and name): αA alpha, βB beta, $\gamma\Gamma$ gamma, $\delta\Delta$ delta, ϵE epsilon, ζZ zeta, ηH eta, $\theta\Theta$ theta, ιI iota, κK kappa, $\lambda\Lambda$ lambda, μM mu, νN nu, $\xi\Xi$ xi, oO omicron, $\pi\Pi$ pi, ρP rho, $\sigma\Sigma$ sigma, τT tau, $\upsilon\Upsilon$ upsilon, $\phi\Phi$ phi, χX chi, $\psi\Psi$ psi and $\omega\Omega$ omega.

- Lots of Greek letters are used in mathematics with different meanings in different contexts. Some are rarely used, in particular, omicron and lots of the capitals are very close or identical to Latin letters and are not used. ξ and ζ are less common because they can be difficult to write, they are sometimes used as small increments in x and z. There are some that are easily confused that are still used, such as ν and κ.

- Sums and products. Say we have a set $X = \{x_0, x_1, x_2, x_3, x_4\}$ then

$$\begin{aligned} \sum_{i=0}^{4} x_i &= x_0 + x_1 + x_2 + x_3 + x_4 \\ \prod_{i=0}^{4} x_i &= x_0 x_1 x_2 x_3 x_4 \end{aligned} \tag{7}$$

  or we might write

$$\begin{aligned} \sum_{x_i \in X} x_i &= x_0 + x_1 + x_2 + x_3 + x_4 \\ \prod_{x_i \in X} x_i &= x_0 x_1 x_2 x_3 x_4 \end{aligned} \tag{8}$$

  and don't be surprised to find

$$\begin{aligned} \sum x_i &= x_0 + x_1 + x_2 + x_3 + x_4 \\ \prod x_i &= x_0 x_1 x_2 x_3 x_4 \end{aligned} \tag{9}$$

  sometimes the bit telling you which x_is are being added or multiplied is left out if it seems obvious what is meant.

Work sheet

1. Use Euler's theorem to calculate

$$3^{81} \pmod{100} \tag{10}$$

2. An enemy organization has encrypted a message with the public key $p = 111$ and $e = 5$; since p is three digits long the message blocks are all taken to be two digits, that is one character, long, with the simple translation of the alphabet into numbers from zero to 25 we have been using. The message is 001101000081025032000109000021000 where each three digits corresponds to the cipher text for one letter. However, by choosing a public key n with less the 2048 bits the enemy organization has made itself vulnerable to a brute force decryption attack, that's your job.

3. This is about encoding rather than decoding, choose two primes that multiply to give a three digit number, chose a exponent 'e' and a short message to encode and encode it. Ideally you should decode it again afterwards.

Exercise sheet

1. Use Euler's theorem to compute

   (a) $3^{340} \pmod{341}$

   (b) $7^{8^9} \pmod{100}$

   (c) $2^{10000} \pmod{121}$

2. Suppose the $n = 10088821$ is the product of two primes and $\phi(n) = 10082272$. What are the prime factors of n?

3. Consider writing a program that implements RSA; the programs on the website called `power.cpp`, `power_faster.cpp` and `rsa_two_digit.cpp` might help.

Challenge

This week's challenge are `projecteuler.net` problems 87 and 97; first one to answer either gets a copy of the book and a kit kat or a handful of choclate, depending on whether they have won before or not.