

# Lab 1: Cipher Fundamentals

**Objective:** The key objective of this lab is to be introduced to some of the fundamental principles involved in cryptography, including the usage of Base-64, hexadecimal, the modulus operator some basic operators (such as AND, OR, X-OR, Rotate Right and Rotate Left), and prime numbers. This lab also involves cracking puzzles, and which have been added to get you to think about the methods involved in cipher cracking. You can undertake the additional lab if you want to further develop your cryptography skills.





 **Web link (Weekly activities):**


[https://github.com/billbuchanan/appliedcrypto/tree/main/unit01\\_cipher\\_fundamentals](https://github.com/billbuchanan/appliedcrypto/tree/main/unit01_cipher_fundamentals)



Go to [vsoc.napier.ac.uk](http://vsoc.napier.ac.uk) and find your folder (Production->CSN11131). Run your **Ubuntu instance** (demo).

**Lab demo:** <https://youtu.be/v6H7lHbIKes> (Note that you will be using Ubuntu, while the demo shows Kali).

## A Introduction [1p]

No	Description	Result
A.1	 <b>Web link (Is prime?):</b> <a href="http://asecuritysite.com/Encryption/testprime">http://asecuritysite.com/Encryption/testprime</a>  Test for the following prime numbers:	91: [Yes] [No] 421: [Yes] [No] 1449: [Yes] [No]
A.2	 <b>Web link (gcd):</b> <a href="http://asecuritysite.com/Encryption/gcd">http://asecuritysite.com/Encryption/gcd</a>  Determine the GCD for the following:	88, 46:  105, 35:
A.3	 <b>Web link (Base-64 convertor):</b> <a href="http://asecuritysite.com/coding/ascii">http://asecuritysite.com/coding/ascii</a>  Determine the Base 64 and Hex values for the following strings:	Hello:  hello:  HELLO:
A.4	 <b>Web link (Base-64 convertor):</b> <a href="http://asecuritysite.com/coding/ascii">http://asecuritysite.com/coding/ascii</a>  Determine the following ASCII strings for these encoded formats:	bGxveWRz  6E6170696572  01000001 01101110 01101011 01101100 01100101 00110001 00110010 00110011

<b>A.5</b>	<p>Using Python, what is the result of 53,431 (mod 453)?</p> <p>In Python, this is:</p> <pre>print (53431 % 453)</pre>	
<b>A.6</b>	<p>Using Python, what is the results of the following:</p> <pre>print (0x43   0x21) print (0x43 &amp; 0x21) print (0x43 ^ 0x21)</pre> <p>Using a pen and paper, prove that these results are correct.</p>	Results:
<b>A.7</b>	<p>Using Python, what is the hex, octal, character, and binary equivalents of the value of 93:</p> <pre>val1=93 print ("Dec:\t",val1) print ("Bin:\t",bin(val1)) print ("Hex:\t",hex(val1)) print ("Oct:\t",oct(val1)) print ("Char:\t",chr(val1))</pre>	Results:
<b>A.8</b>	<p>JavaScript is often used in cryptography. Using node.js, repeat A.7.</p> <pre>val=93 console.log(val.toString(2)) console.log(val.toString(16)) console.log(val.toString(8)) console.log(String.fromCharCode(val))</pre> <p>This program will use node.js. Create a file named a_08.js and then run with:</p> <pre>node a_08.js</pre>	Results:
<b>A.9</b>	<p>Using Python, what is the Base-64 conversion for the string of “crypto”?</p> <pre>import base64 str="crypto" print base64.b64encode(str.encode())</pre>	Result:
<b>A.10</b>	<p>If we use a string of “crypto1”, what do you observe from the Base64 conversion compared to the result in the previous question (A.9)?</p>	Observation:
<b>A.11</b>	<p>Using Python, using a decimal value of 41, determine the result of a shift left by one bit, a shift left by two bits, a right shift by one bit, and a right shift by two bits:</p> <p> <b>Web link (Bit shift):</b>  <a href="https://asecuritysite.com/comms/shift">https://asecuritysite.com/comms/shift</a></p>	<p>Decimal form: 41  Shift left (1):  Shift left (2):  Shift right(1):  Shift right(2):</p> <p>Why would a shift left or shift right operator not be</p>

		used on its own in cryptography?
A.12	<p>In several cases in cryptography, we try and factorize a value into its factors. An example is 15, and which has factors of 5 and 3. Using the Python program defined in the following link, determine the factors of 432:</p> <p> <b>Web link (Factorization):</b>  <a href="https://asecuritysite.com/encryption/factors">https://asecuritysite.com/encryption/factors</a></p> <p>Think of two extremely large values and determine their factors.</p>	
A.13	<p>Another format we can use for our data is compression, and we can do the compression before or after the encryption process. One of the most popular methods is gzip compress, and which uses the LZ method to reduce the number of bits used. For this we will use node.js. Create a file named a_13.js and determine what the following Base64 conversions are when they are uncompressed (Hint: they are cities of the World):</p> <p> <b>Web link (Compression):</b>  <a href="https://asecuritysite.com/encryption/gzip">https://asecuritysite.com/encryption/gzip</a></p> <p>Take a string of “abc” and compress it, and now keep building up the string with the same sequence (such as “abcabc...”). What do you observe from the length of the compression string if you use a random characters of the same length as an input:</p>	eJzzyc9Lyc8DAAgpAms= eJxzSi3KycWDAAfXA10= eJzzSy1XiMwvygYADKUC8A==

Note: The code in this example uses Python 2.7. If you are using Python 3, remember and put parenthesis around the print statement string, such as `print (hex(val))`.

## B GCD [1p]

GCD is known as the greatest common divisor, or greatest common factor (gcf), and is the largest positive integer that divides into two numbers without a remain-der. For example, the GCD of 9 and 15 is 3. It is used many encryption algorithms, and a sample algorithm to determine the GCD of two values (a and b) is given on:

 **Web link (GCD):** <http://asecuritysite.com/encryption/gcd>

No	Description	Result
B.1	Write a Python program to determine the GCD for the following:	4105 and 10:  4539 and 6:
B.2	Two numbers are co-prime if they do not share co-factors, apart from 1, which is $\text{gcd}(a,b)=1$ .  Determine if the following values are co-prime:	5435 and 634: Yes/No  5432 and 634: Yes/No

## C Modulus and Exponentiation [1p]

The **mod** operator results in the remainder of an integer divide. For example, 31 divided by 8 is 3 remainder 7, thus  $31 \bmod 8$  equals 7. Often in cryptography the mod operation uses a prime number, such as:

Result =  $\text{value}^x \bmod (\text{prime number})$

For example, if we have a prime number of 269, and a value of 8 with an  $x$  value of 5, the result of this operation will be:

Result =  $8^5 \bmod 269 = 219$

With prime numbers, if we know the result, it is difficult to find the value of  $x$  even though we have the other values, as many values of  $x$  can produce the same result. It is this feature which makes it difficult to determine a secret value (in this case the secret is  $x$ ).

Exponentiation ciphers use a form of:

$$C = M^e \bmod p$$

to encrypt and decrypt a message ( $M$ ) using a key of  $e$  and a prime number  $p$ .

No	Description	Result
C.1	What is the result of the following:	$8^{13} \bmod 271$ :  $12^{23} \bmod 973$ :
C.2	Implement a Python program which will determine the result of:  $M^e \bmod p$  The program should check that $p$ is a prime number.	Is the result of $8^5 \bmod 269$ equal to 219?  Yes/No

<b>C.3</b>	<p>Now prove the following:</p> <p>(a) message = 5, e=5, p = 53. Ans: 51</p> <p>(b) message = 4, e=11, p = 79. Ans: 36</p> <p>(c) message = 101, e=7, p = 293. Ans: 176</p> <p>An outline of the Python code is:</p> <pre> message = raw_input('Enter message: ') e = raw_input('Enter exponent: ') p = raw_input('Enter prime ')  cipher = (int(message) ** int(e)) % int(p) print cipher </pre>	<p>Have you proven the answers:</p> <p>(a) Yes/No</p> <p>(b) Yes/No</p> <p>(c) Yes/No</p>
------------	---	---

## Advanced Lab

The rest of the lab are more advanced applications, and are only added for those looking for additional challenges.

### D Simple prime number test [2p]

A prime number is a value which only has factors of 1 and itself. Prime numbers are used fairly extensively in cryptography, as computers struggle to factorize them when they are multiplied together. The simplest test for a prime number is to divide the value from all the integers from 2 to the value divided by 2. If any of the results leaves no remainder, the value is a prime, otherwise it is composite. We can obviously improve on this by getting rid of even numbers which are greater than 2, and also that the highest value to be tested is the square root of the value.

So, if  $n = 37$ , then our maximum value will be  $\sqrt{n}$ , which, when rounded down is 6. So, we can try: 2, 3, and 5, of which none of these divide exactly into 37, so it is a prime number. Now let's try 55, we will then be 2, 3, 5 and 7. In this case 5 does divide exactly in 55, so the value is not prime.

Another improvement we can make is that prime numbers (apart from 2 and 3) fit into the equation of:

$$6k \pm 1$$

where  $k=0$  gives 0 and 1,  $k=1$  gives 5 and 7,  $k=2$  gives 11 and 13,  $k=3$  gives 17 and 19, and so on. Thus we can test if we can divide by 2 and then by 3, and then check all the numbers of  $6k \pm 1$  up to  $\sqrt{n}$ .

 **Web link (Prime Numbers):** <http://asecuritysite.com/encryption/isprime>

No	Description	Result
D.1	Using the equation of $6k \pm 1$ . Determine the prime numbers up to 100:	Prime numbers:
D.2	Implement a Python program which will calculate the prime numbers up to 1000:	Define the highest prime number generated:

A prime sieve creates all the prime numbers up to a given limit. It progressively removes composite numbers until it only has prime numbers left, and it is the most efficient way to generate a range of prime numbers. The following provides a fast method to determine the prime numbers up to a given value (test):

```
import sys
test=1000
if (len(sys.argv)>1):
    test=int(sys.argv[1])
def sieve_for_primes_to(n):
```

```


size = n//2
sieve = [1]*size
limit = int(n**0.5)
for i in range(1,limit):
    if sieve[i]:
        val = 2*i+1
        tmp = ((size-1) - i)//val
        sieve[i+val::val] = [0]*tmp
return [2] + [i*2+1 for i, v in enumerate(sieve) if v and i>0]

```

```
print (sieve_for_primes_to(test))
```

No	Description	Result
<b>D.3</b>	Implement the Python code given above and determine the highest prime number possible in the following ranges:	Up to 100:  Up to 1,000:  Up to 5,000:  Up to 10,000:

The Miller-Rabin Test for Primes is an efficient method in testing for a prime number. Access the following page and download the Python script.

 **Web link (Miller-Radin):** <http://asecuritysite.com/encryption/rabin>

Using this determine the following:

No	Description	Result
<b>D.4</b>	Which of the following numbers are prime numbers:	Is 5 prime? Yes/No  Is 7919 prime? Yes/No  Is 858,599,509 prime? Yes/No  Is 982,451,653 prime? Yes/No  Is 982,451,652 prime? Yes/No


## E Random numbers [2p]

Within cryptography random numbers are used to generate things like encryption keys. If the generation of these keys could be predicted in some way, it may be possible to guess it. The two main types of random number generators are:

- **Pseudo-Random Number Generators (PRNGs).** Repeats after a given time. Fast. They are also deterministic and periodic, so that the random number generation will eventually repeat.
- **True Random Number Generators (TRNGs).** This method is a true random number such as for keystroke analysis. It is generally slow but is non-deterministic and aperiodic.

Normally simulation and modelling use PRNG, so that the values generated can be repeated each time, while cryptography, lotteries, gambling and games use TRNG, as each value which is selected at random should not repeat or be predictable. In the generation of encryption keys for public key encryption, a user is typically asked to generate some random activity with their mouse pointer. The random number is then generated on this activity.

Computer programs often struggle to generate TRNG, and hardware generators are sometimes used. One method is to generate a random number based on low-level, statistically random "noise" signals. This includes things like thermal noise, and a photoelectric effect.

 **Web link (Random number):** <http://asecuritysite.com/encryption/random>

One method of creating a simple random number generator is to use a sequence generator of the form (Linear Congruential Random Numbers):

$$X_{i+1} \leftarrow (a \times X_i + c) \bmod m$$

Where a, c and m are integers, and where  $X_0$  is the seed value of the series.

If we take the values of  $a=21$ ,  $X_0=35$ ,  $c=31$  and  $m=100$  we get a series of:

66 17 88 79 90 21 72 43 34 45 76 27 98 89 0 31 82 53
--

Using this example, we get:

$(21 \times 35 + 31) \bmod 100$  gives 66  
 $(21 \times 66 + 31) \bmod 100$  gives 17  
 $(21 \times 17 + 31) \bmod 100$  gives 88  
and so on.

 **Web link (Linear congruential):** <http://asecuritysite.com/encryption/linear>

No	Description	Result
E.1	Implement the Python code given above.	Does it generate this sequence?
	Using: $a=21$ , seed=35, $c=31$ , and $m=100$ , prove that the sequence gives 66 17 88 79 90	Yes/No



<b>E.2</b>	Determine the sequence for:  a=22, seed=35, c=31, and m=100.	First four numbers of sequence?
<b>E.3</b>	Determine the sequence for:  a=954,365,343, seed=436,241, c=55,119,927, and m=1,000,000.	First four numbers of sequence?
<b>E.4</b>	Determine the sequence for:  a=2,175,143, seed=3553, c=10,653, and m=1,000,000.	First four numbers of sequence?

**Xoroshiro128+** is one of the fastest Pseudorandom number generators (PRNGs). It was created in 2016 by David Blackman and Sebastiano Vigna and requires two 64-bit unsigned integers as seeds:

<https://asecuritysite.com/encryption/xoro>

Using the Python program to select Head or Tails, create a run for 500 tosses (perhaps running it a few times and noting the balance of Heads and Tails), and show that program is unlikely to be biased towards Heads or Tails?

## F Breaking the Shift Cipher [1p]

In this exercise, you will practice decrypting messages encrypted using the shift cipher. Through a step-by-step process, you will explore the effectiveness of a brute force attack in deciphering messages when the key is unknown.

### 1. Decrypting with Brute Force

- **Given Ciphertext:** Obtain the ciphertext provided in the lab material.
- **Brute Force Attack:** You will decrypt the ciphertext using a brute force attack. Use each of the twenty-six different keys ( $k=0, 1, \dots, 25$ ) to decrypt the message.
- **Decrypt the ciphertext** using key  $k=0$  and record the corresponding plaintext.
- Continue this process for keys  $k=1$  to  $k=25$ , noting the decrypted plaintexts for each key.
- **Observing Plaintexts:** Review the decrypted plaintexts you obtained in the previous step.
- **Selecting the Correct Plaintext:** Choose the most appropriate plaintext that appears to be meaningful English text. This will be your recovered plaintext.
- **Verification:** Verify the accuracy of your answer by encrypting the solution plaintext using your chosen key and checking if it matches the original ciphertext.

### 2. Automate a brute force attack

- Write a code to automate a brute force attack for the shift cipher encryption. Your code should:
  - Take the ciphertext and iterate through all possible key values (0 to 25).
  - For each key, decrypt the ciphertext using the key and print the resulting plaintext.
  - Determine the most meaningful plaintext among the results.
  - Display the recovered plaintext along with the corresponding key that produced it.

### 3. Decrypt the following ciphertext using a brute force attack

- ymnx nx ymj ktwjxy uwnrjafq
- esp bflwtej zq xpcnj td yze decltypo}
- owlzwhghdwgxlzwmfalwvklslwk
- haahjr ha khdu
- wkh srufxslqh lv xqghu wkh vkhhwv
- WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

## G Breaking the Mono-alphabetic Substitution Cipher [2p]

In this exercise, you will explore the vulnerabilities of the mono-alphabetic substitution cipher and learn how to break it using frequency analysis. Through a step-by-step process, you'll decipher a ciphertext encrypted using this cipher and reveal the original plaintext message.

Here is the table of frequencies of English alphabets for your reference:

a	b	c	d	e	f	g	h	i	j	k	l	m
8.167	1.49	2.782	4.253	12.702	2.228	2.015	6.094	6.966	0.153	0.772	4.025	2.406
n	o	p	q	r	s	t	u	v	w	x	y	z
6.749	7.507	1.929	0.095	5.987	6.327	9.056	2.758	0.978	2.360	0.150	1.974	0.074

**Decrypting the following ciphertext:**

lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi  
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx  
ymbnlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr  
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwj  
lmird jk xjubt trmui jx ibndt

wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkbi mkd wbi  
iwokwxwvmkv mkd ijyr ynib urymwk nkrashmwkrd bj ower m  
vjyshrbr rashmkmbwj jkr cjhnd pmer bj lr fnmhwswrd mkd  
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr  
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrri  
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh  
mnbpjuwbt lnb yt rasruwrkv cwbp qmbm pmi hrxb kj djnlb  
bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwj mkd  
wkbrusurbmbwj w jxxru yt bprjuwri wk bpr pjsr bpmb bpr  
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvp

1. Compute the relative frequency of all letters A...Z in the ciphertext. You may want to use a tool such as the open-source program CrypTool for this task. However, a paper and pencil approach is also still doable.
2. Decrypt the ciphertext with the help of the relative letter frequency of the English language. Note that the text is relatively short and that the letter frequencies in it might not perfectly align with that of general English language from the table.

## H What I should have learnt from this lab?

---

The key things learn:

- Some fundamental principles around number and character formats, including binary, hexadecimal and Base64.
- How to run a Python program and change some of the parameters.
- Some fundamentals around prime numbers , mod operations, Shift Cipher and Breaking the Mono-alphabetic Substitution Cipher.

## Notes

---

The code can be downloaded from:

```
git clone https://github.com/billbuchanan/appliedcrypto
```

If you need to update the code, go into the appliedcrypto folder, and run:

```
git pull
```

To install a Python library use:

```
pip install libname
```

To install a Node.js package, use:

```
npm install libname
```

## Possible solutions

---

Have a look at: [https://github.com/billbuchanan/appliedcrypto/tree/main/z\\_solutions](https://github.com/billbuchanan/appliedcrypto/tree/main/z_solutions)

Many of the key concepts in cryptography are based on number theory and which is the study of integers, with a special focus on divisibility. The main classifications for numbers are integers, rational numbers, real numbers and complex numbers. In maths we define these as:

- Integers can be positive or negative numbers and have no fractional part. They are represented with the  $\mathbb{Z}$  symbol  $\{\dots-2, -1, 0, +1, +2, \dots\}$ . A special case of this is finite cyclic group ( $\mathbb{Z}_p$ ), and which represents the integer values from 0 to  $p-1$ , and where  $p$  is a prime number. This is cyclic as we take  $(\text{mod } p)$  of our values.
- Rational numbers are fractions ( $\mathbb{Q}$ ).
- Real numbers ( $\mathbb{R}$ ) include both integers and rational numbers, and any other number that can be used in a comparison.
- Prime numbers ( $\mathbb{P}$ ) represent the integers which can only be divisible by itself and unity.
- Natural numbers ( $\mathbb{N}$ ) represent positive numbers which are integers  $\{1, 2, \dots\}$ .

One of the great advantages of using Python is that it automatically casts to big integers.