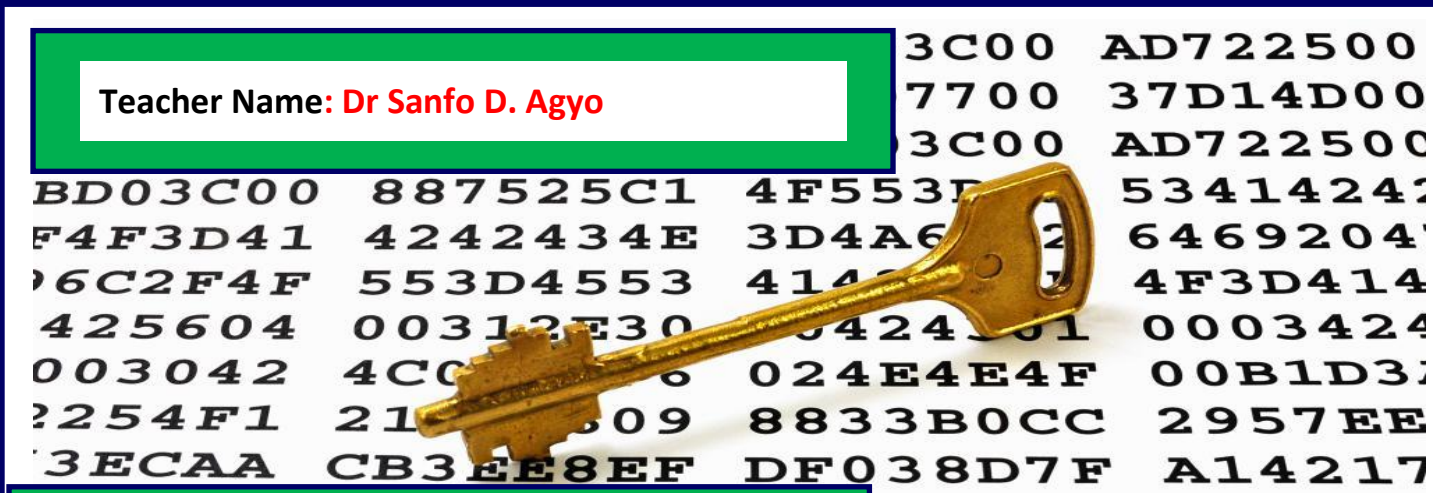
Type equation here.

PROTECTING INFORMATION USING MATHEMATICS

Key Stage 4 Programme – 2016-2017

Teacher Name: Dr Sanfo D. Agyo



Pupil Name_____

Timetable and Assignment Submission

Fill this in with your teacher.

Timetable – Tutorials

Tutorial	Date	Time	Location
1			PHS
2			PHS
3			PHS
4			PHS
5			PHS
6			PHS

Timetable – Homework Assignments

Homework Assignment	Description	Due Date
Tutorial 1	Basic Mathematics for cryptography	
Tutorial 2	Symmetric encryption	
Tutorial 3	Affine and modulo arithmetic	
Tutorial 4	Asymmetric encryption: RSA I	
Tutorial 5	Asymmetric encryption: RSA II	

Assignment Submission – Lateness and Plagiarism

Lateness	
Submission after 4.00pm on **Put date here**	10 marks deducted
Plagiarism	
Some plagiarism	10 marks deducted
Moderate plagiarism	20 marks deducted
Extreme plagiarism	Fail

KS4 Programme 2016-17 – Pupil Feedback Report

Grade	Marks	What this means
1st	70+	Performing to an excellent standard at A-Level
2:1	60-69	Performing to a good standard at A-Level
2:2	50-59	Performing to an excellent standard at current key stage
3rd	40-49	Performing to a good standard at current key stage
Working towards a pass	0-39	Performing below a good standard at current key stage
Did not submit	DNS	No assignment received by The Brilliant Club

Lateness	
Any lateness	10 marks deducted
Plagiarism	
Some plagiarism	10 marks deducted
Moderate plagiarism	20 marks deducted
Extreme plagiarism	AuJeffatic fail

Name of RIS Teacher	Dr Sanfo Agyo		
Title of Assignment	Protecting information using Mathematics		
Name of Pupil			
Name of School	Parliament Hill School Camden		
ORIGINAL MARK / 100		**FINAL MARK / 100**	
DEDUCTED MARKS		**FINAL GRADE**	

If marks have been deducted (e.g. late submission, plagiarism) the teacher should give an explanation in this section:

Learning Feedback Comment 1 - *Enter Key Learning Priority Here*	
What you did in relation to this Key Learning Priority *Enter feedback here*	**How you could improve in the future** *Enter feedback here*
Learning Feedback Comment 2 – *Enter Key Learning Priority Here*	
What you did in relation to this Key Learning Priority *Enter feedback here*	**How you could improve in the future** *Enter feedback here*
Learning Feedback Comment 3 – *Enter Key Learning Priority Here*	
What you did in relation to this Key Learning Priority *Enter feedback here*	**How you could improve in the future** *Enter feedback here*
Resilience Comment	
How you showed learning resilience during the course *Enter feedback here*	**How you could build learning resilience in the future** *Enter feedback here*

Example

Contents

Course Rationale…… Page 5

Course map……...Page 7

Mark Scheme……...Page 8

Glossary of Keywords…….....Page 7

Tutorial 1……..…Page x

- Activity 1……Page x
- Activity 2……Page x
- Activity n……Page x
- Tutorial 1 Homework – Baseline Test……Page x

Tutorial 2……Page x

- Activity 1……Page x
- Activity 2……Page x
- Activity n……Page x

Tutorial 3……Page x

- Activity 1……Page x
- Activity 2……Page x
- Activity n……Page x

Tutorial 4……Page x

- Activity 1……Page x
- Activity 2……Page x
- Activity n……Page x

Tutorial 5……Page x

- Activity 1……Page x
- Activity 2……Page x
- Activity n……Page x

Appendix 1: Referencing……Page x

Appendix 2: University Application

Guidance……Page x

Course Rationale

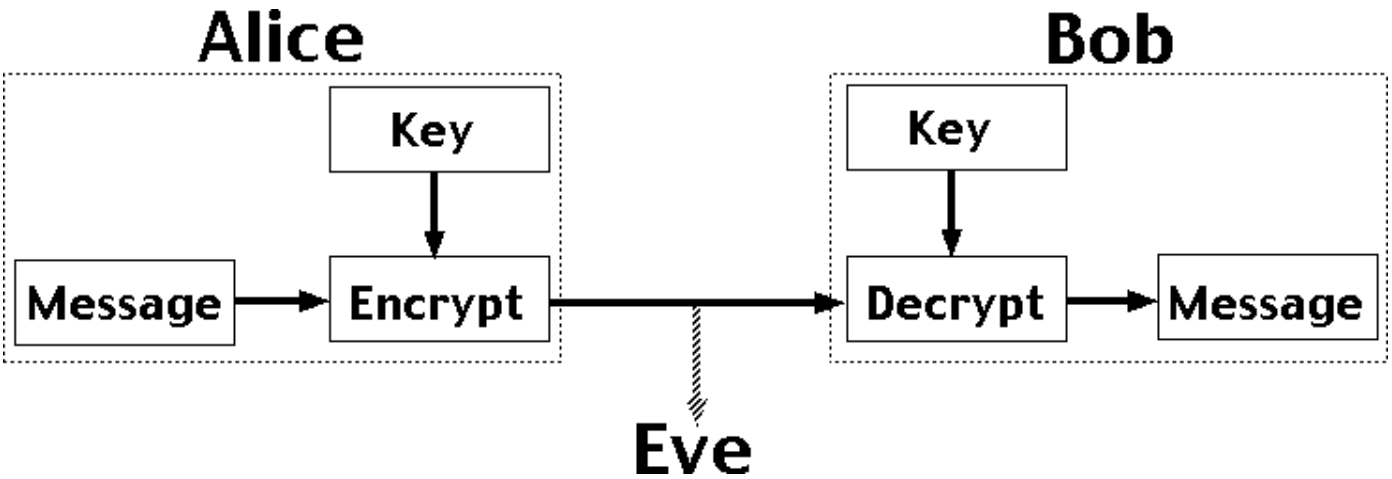
The concept of information hiding has been in existence as far back as 1900 BC in ancient Egypt. There are early accounts of monarchs encrypted messages so that even if intercepted cannot be interpreted to the common user.

During World war II and the Enigma cracking

In modern times, encryption and security in general focuses on three majors: confidentiality, integrity and authentication. Confidentiality refers to the case where critical information is only available to the right parties and anyone who is not authorised should neither have access nor be in a position to even understand the message. Integrity on the other hand considers the original message is not modified during the course of transmission from sender Alice to receiver Bob. If for any reason an intruder called Eve can intercept the message, decrypts, modify it and retransmit it to Eve, then integrity is compromised. Lastly, authentication is a build-up on integrity, where the receiver can for sure confirm that what is received is what was actually sent.

The tutorials will consider the basic components of encryption with more focus on message confidentiality such that a plaintext (a readable English text) is encrypted using different methods to give a ciphertext (encrypted message).

Formally we define encryption as an encoding of plaintext into ciphertext such that it is unreadable to an unauthorised party. A diagrammatic representation of encryption is shown below where Alice intends to send a message to Bob. First she encrypts the message using a secret key and sends the message to Bob. The key could have been agreed before hand with Bob so that both of them have the same key. Bob receives the message and because it is presumed only both of them have the key, Bob decrypts the ciphertext and reads the message. Eve is an intruder who can intercept the message but will hopefully be unable to read the message because she doesn't understand it (Eve doesn't have the key).



If a single key is used by Alice to encrypt and Bob to decrypt the message, this category of encryption is called Asymmetric encryption. We shall be exploring many cases of asymmetric encryption in the next few tutorials. However, there are cases where one key is used by Alice to encrypt and a different key is used by Bob to decrypt. This is called asymmetric encryption and is obviously a better kind of encryption.

In this course, we shall consider the following:-

A. **Symmetric**
    1. **Shift cipher**
    2. **Substitution ciphers/transposition: single, Vigenere**
    3. **Enigma case study (School trip)**
B. **Asymmetric encryption: RSA case study**

And the course will be structured such that:-

Week 1: Mathematics of primes and number patterns

Week 2: Shift and substitution ciphers

Week 3: Affine codes/Modulo arithmetic with N/extended euclid

Week 4: RSA encryption I

Week 5: RSA encryption II

Week 6: Review

Course Map

Basic Mathematics for cryptography
Symmetric encryption: Mono-alphabetic
Affine and modulo arithmetic
Encryption using RSA and substitution cipher
RSA encryption I
RSA encryption II

Glossary of Keywords

Word	Definition	In a sentence…
Prime numbers		
Coprime		
Plaintext		
Ciphertext		
Eavesdropping		
Encryption key		
Symmetric encryption		
Assymetric encryption		
Public key		
Private key		

Tutorial 1 – Basic mathematics of cryptography

Today's Key Question(s):

- Why do we study mathematics? Does it have any relation to my life?
- How are patterns used in mathematics?

What is the Purpose of Tutorial 1?

- To consider some basic mathematics concepts necessary for cryptography.
- To understand the relevance of number patterns.

Patterns and Prime numbers

The beauty of mathematics is that it reveals patterns. Imagine a sequence of numbers:
a). 1, 4, 7, 10, 13, 16, 19, 22, 25,…..
b). 19, 27, 35, 43,…..
c). 1, 2, 4, 8, 16, 32, 64, 128, 256,…
d). 1, 4, 9, 16, 25, 36, 49,……
e). 1, 8, 27, 64, 125,….

Imagine we consider numbers like 1, 3, 5, 7, 11, 19, 23, 29, 31, 53, 61, 89, 113, 1009……. Do you observe any pattern in these numbers?

If you guessed right, then you would have observed that they are prime numbers. Prime numbers in the words of Marcus du Sautoy are the lynchpin for security and e-commerce. This includes protecting our details when we are on Instagram or any social media platform, securing online transactions etc. Prime numbers come in very handy in all these scenarios and many more.

Every number that is not a prime can be constructed by multiplying prime numbers together.

Basic mathematics concepts used in cryptography

Modular arithmetic (Modulus)

The modulus considers the remainder when a number divides another.

$$\frac{A}{B} = C \; remainder \; D$$

A divides B to give C and D is the remainder.

In this case fractions are never the case. The symbol for modulus we will be using is '%' or MOD. Conventionally, we write it as,

MOD (A, B) = D

For example, consider 4 % 2 or MOD (4,2), the answer for both is 0. This is because 4 divides 2 to give 2 without any remainder. Another can be MOD (64,5), the answer is 4 because the closest factor of 5 to 64 is 60 with a remainder of 4.

Can you guess, MOD (175,7) = ?.

GCD (Greatest Common divisor)

Imagine we have two numbers 24 and 48, the greatest common divisor will be the greatest common factor (HCF) which will be 24.
Mathematically, it is written as,

$$\gcd(24,48) = 24$$

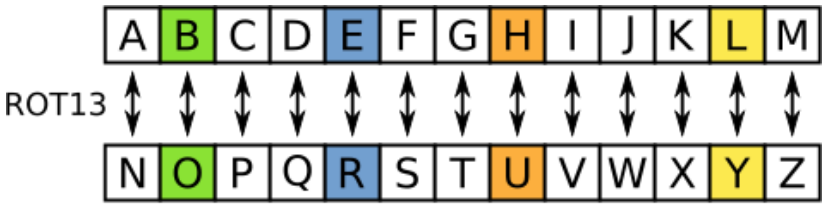
The concept is very similar to that of Highest Common Factor (HCF).
It will therefore not be too strange to think that for a prime number the greatest common divisor is 1 and itself.

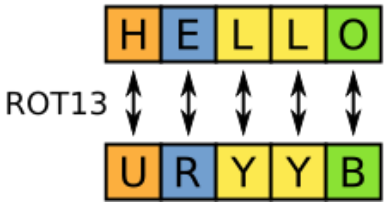
HOMEWORK

1. Find the missing terms for each of the questions below: -
   i) $1, 6, 81, 256, ?, ?$
   ii) $1, 3, 6, 10, ?, ?$
   iii) $(1,1) \rightarrow \sqrt[2]{2}, (6,8) \rightarrow 10, (3, x) \rightarrow \sqrt[2]{10}, (x + 5,2) \rightarrow \sqrt[2]{53}$
   iv) $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ?, ?$
2. Find the missing terms from the series shown below:
   i) $1, 2, 4, 6, 10, 12, 22, 28, 36, 40, ?, ?$
   ii) $10, 15, 25, 35, 55, 85, 95, 115, ?, ?$
   iii) $4, 16, 37, 58, ?, ?, 42, 20, 4, 16, 37, 58, ?, ?, 42, 20, 4$
   iv) $1, 2, 10, ?, 101, 226, ?, 785, ?, 2026$
3. Find the Greatest Common Divisors (GCDs) of the following: -
   i) gcd (220,1323)
   ii) gcd (1424,3084)

iii) gcd (406,555)
iv) gcd $(4278, 8602)$

Tutorial 2 – Mono-alphabetic encryption (Shift & transpositional ciphers)





Today's Key Question(s):

- How was early cryptography performed?
- What were some of the loopholes in these early cryptography techniques?

What is the Purpose of Tutorial 2?

- To understand how shift ciphers work and consider examples.
- To understand substitution ciphers with examples

Historical background

The shift Caesar was used in early days of encryption based on very simple logic where a certain number shifted the 26 letters of the alphabet.
Imagine a case where Alice wants to send a message to Bob and she uses the shift order of 3, the mapping is shown below:-

$$\frac{A}{X}\ \frac{B}{Y}\ \frac{C}{Z}\ \frac{D}{A}\ \frac{E}{B}\ \frac{F}{C}\ \frac{G}{D}\ \frac{H}{E}\ \frac{I}{F}\ \frac{J}{G}\ \frac{K}{H}\ \frac{L}{I}\ \frac{M}{J}\ \frac{N}{K}\ \frac{O}{L}\ \frac{P}{M}\ \frac{Q}{N}\ \frac{R}{O}\ \frac{S}{P}\ \frac{T}{Q}\ \frac{U}{R}\ \frac{V}{S}\ \frac{W}{T}\ \frac{X}{U}\ \frac{Y}{V}\ \frac{Z}{W}$$

This shift order is also called the key, thus we have the equation,

Ciphertext = plaintext + key (3)

Activity
Write the equation for the plaintext in terms of the ciphertext and key.

EXAMPLE 1
Typically, to encrypt a plaintext message say THERESA MAY will be done by

$$\begin{array}{ccccccc} T & H & E & R & E & S & A \\ \hline Q & E & B & O & B & P & X \end{array} \qquad \begin{array}{ccc} M & A & Y \\ \hline J & X & V \end{array}$$

Therefore, in technical terms we say that,

Plaintext: THERESA MAY
Ciphertext: QEBOBPX JXV

The ciphertext is the message Alice will transmit over a transmission line or network. Bob receives the message and should have known that the key is 3, and using the key decrypts the message.

Activity
Discuss is there any possibility of knowing the plaintext from the ciphertext? If this is possible, then the attack on the ciphertext to get the plaintext is called **ciphertext attack.**

EXAMPLE 2
Encrypt the message “I AM SPECIAL”. Give it as a ciphertext without spaces.

Limitations of Mono-alphabetic encryption

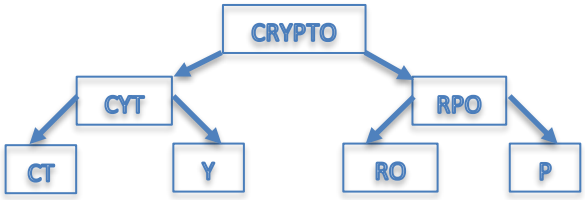
HOMEWORK

1. Alice is in France in 1875 and writes a letter to her son Bob who is a cryptographer. She is trying to test his knowledge of shift cipher and sends him a message that is partly German and English. The ciphertext sent by Alice is shown below:

```
JQRRG, JQRRG, TGKVGT
JQRRG, JQRRG, TGKVGT,
YGPP GT HCGNNV, FCPP UEJTGKV GT. HCGNNV GT KP
FGP ITCDGP, HTGUUGP KJP FKG TCDGP,
HCGNNV GT KP FGP UWORH,
FCPP OCEJV FGT TGKVGT RNWORU!
JWORVA FWORVA
JWORVA FWORVA UCV QP C YCNN
JWORVA FWORVA JCF C ITGCV HCNN
CNN VJG MKPI'U JQTUGU CPF CNN VJG MKPI'U OGP
EQWNFP'V RWV JWORVA VQIGVJGT CICKP.
```

2. This exercise is called the Beaver code. The logic begins by first deleting all spaces from the plaintext in order to encrypt it with the Beaver Code. Afterwards, the plaintext is divided into two parts. The left half contains all letters that are on an odd position in the plaintext; in the right half all-even letters are collected. The resulting parts are divided according to this rule until each part is no longer than two letters. These parts are merged from left to right.

Take an example



Thus,

Plaintext: CRYPTO
Ciphertext: CTYROP

Decrypt the ciphertext, **TTRNEHEORAVNEWESEAABBTREOT**.

In order to solve the challenge, you need to decrypt the English sentence, insert spaces at the correct positions and enter the sentence in capital letters (without punctuation marks).

Tutorial 3

Affine codes/Modulo arithmetic with N/extended euclid

Today's Key Question(s):

- How is modular arithmetic introduced in tutorial 1 used in cryptography?

What is the Purpose of Tutorial 4?

- Introduce modular arithmetic as a stepping stone towards RSA encryption in
- To apply the concept of modular arithmetic in encryption.

Kirsty and Caroline are 14-year-old girls who attend Parliament Hill School in Camden. They love to chat with each other and talk about the important things in life, for example latest fashion, movies and events in London. Once, Caroline's mom read Caroline's messages and as a result Caroline's parents asked many questions. Now the two girls are thinking about a solution to make this awkward situation never happen again. They ask their best friend Jeff for a hint as he regularly reads 'Sherlock Holmes' and 'The Three Investigators' and is very keen on cryptography in his spare time. The affine cipher comes to Jeff's mind. It describes a possibility to encrypt single letters to obfuscate the meaning of a text.

Jeff's idea in detail:

1. The English alphabet consists of 26 letters.
2. Each plaintext letter is mapped by a rule to a ciphertext letter. For that, each letter is represented as a number within {0,1,2,3, ... 23,24,25}. The rule to encrypt a plaintext letter x to a ciphertext letter y is:

$$y = (a \cdot x + b) \bmod 26$$

3. a, b are the parts of the secret key, which Caroline and Kirsty should not tell anybody. They both decide that ‘a’ and ‘b’ be prime numbers.
4. The key consists of the following numbers: a = 17, b = 7.

Jeff makes a final rehearsal before he presents his proposal to Caroline and Kirsty. He encrypts a text and gets:

Ciphertext: GNXB NBS XNUX FXWXNDX UHPWKNPWS

Plaintext: D

The plaintext letter D is represented by the value x = 3. Therefore y is calculated by y = (17 · 3 + 7) mod 26 = 58 mod 26 = 6, representing G.

Now Jeff realized, that he has not thought yet about the decryption of the message. He is short on time and overdue with his suggestion.

Support Jeff by finding a way to decrypt the ciphertext. Reveal the meaning of the shown example and hand it in as solution. Please use only capital letters.

HINT:

$$6 = 6 \; mod \; 26 = \; 58 \; mod \; 26 = 84 \; mod \; 26$$
$$17^{-1} mod \; 26 = 23$$

1. $y \; = \; 17x \; + \; 7 \; mod \; 26$

2. $17x \; = \; y \; - \; 7 \; mod \; 26$

3. $x \; = \; (y \; - \; 7)/17 \; mod \; 26$

4. $x \; = \; y/17 - 7/17 \; mod \; 26$

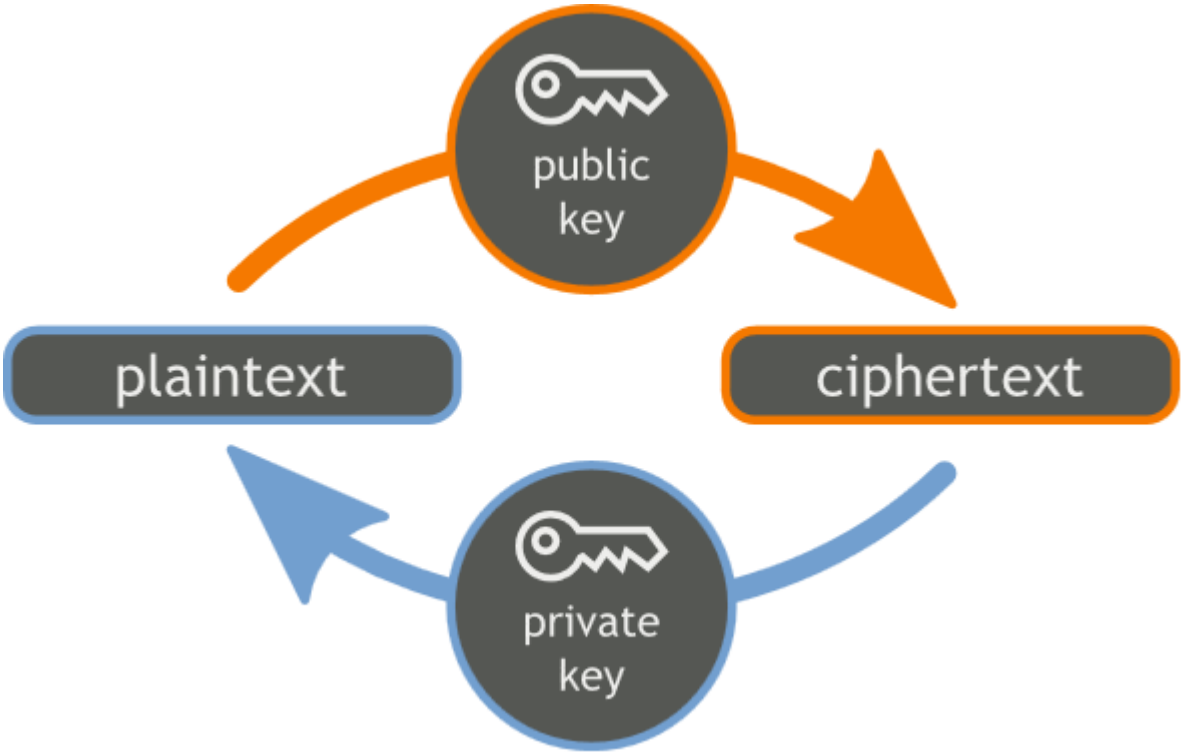
5. $(23 \; = \; 17^{-1} \; mod \; 26, because \; 23 \; x \; 17 \; = \; 1 \; mod \; 26)$

6. $x \; = \; 23y - 7 \; x \; 23 \; mod \; 26$

7. $x \; = \; 23y \; + \; 21 \; mod \; 26$

Tutorial 4

Encryption in modern science- RSA part I



Today's Key Question(s):

- How is encryption used in modern day science?
- What makes an encryption standard secure?
- Key generation of RSA.

What is the Purpose of Tutorial 3?

- To detail some modern examples of encryption and how they are used.
- To understand the application of encryption in securing internet data and transaction.

Introduction to RSA

All the encryption protocols we viewed previously were based on using a single key for both encryption and decryption. This type of encryption is called Symmetric cryptography. However, it is possible to have two different keys mathematically related to each other so that one can be used for encryption and another for decryption. This type of encryption is called Asymmetric cryptography. A typical example of such encryption protocol is the RSA.

RSA encryption was developed by two computer scientists Ronald Rivest and Adi Shamir, along with number theorist Leonard Adleman and RSA bears their initials (Rivest, Shamir and Adleman). RSA is widely used for encrypting Internet credit-card transactions, securing e-mail, and authenticating phone calls.

Assume we call the key for encryption ***e,*** and the decryption key ***d,*** RSA is implemented such that the encryption key ***e*** (also called public key) is made public for anyone to use but the decryption key, ***d*** (also called private key) is hidden from the public.
The protocol is secured because the keys are related mathematically but the computation is such that it is impossible or seemingly expensive to calculate the private key from the public key.

RSA protocol description

RSA protocol involves three stages: -
1. Key generation
2. Encryption
3. Decryption

Stage 1: Key generation

The effectiveness and security of RSA is based on the factoring problem. **The factoring problem is factorising a number into prime factors.** This can be easy for small numbers, e.g., 391 = 23 x 17, but for large numbers, it is either incredibly hard to decompose or very expensive.

Step 1: Select two prime numbers (large primes in real applications), let's call them ***p*** and ***q*** at random.

Step 2: Compute **n = pq.** This product **n** will be used as the modulus for both the public key and private key.

Step 3: Compute $\varphi(n) = (p-1)(q-1)$ where φ is Euler's totient function.

Step 4: Choose an integer ***e,*** such that $1 < e < \varphi(n)$ and $\gcd\big(e, \varphi(n)\big) = 1$
The number e is the public key released for anyone to use.

Step 5: Determine ***d*** (decryption key) such that it is the multiplicative inverse of ***e*** by, $\boldsymbol{d \equiv e^{-1} mod\ \varphi(n)}$ or $\boldsymbol{(d \times e)\ mod\ \varphi(n) = 1}$.

In real applications, the pair $(\boldsymbol{n}, \boldsymbol{e})$ are made public and called the **public key component.** The other pair **(n, d)** are called the **private key** component. Also, **p, q and** $\boldsymbol{\varphi(n)}$ are also kept secret so that **d** cannot be calculated.

Example 1

Step 1: Choose $p = 3$ and $q = 11$

Step 2: Compute $n = pq = 3 \times 11 = 33$

Step 3: $\varphi(n) = (p-1) \times (q-1) = 2 \times 10 = 20$

Step 4: Select the encryption key ***e,*** such that, $1 < e < \varphi(n)$, $\gcd\big(e, \varphi(n)\big) = 1$. Let $\boldsymbol{e} = 7$

Step 5: Compute ***d,*** such that $\boldsymbol{(d \times e)\ mod\ \varphi(n) = 1}$.
d can be 3, since $(3 \times 7) mod\ 20 = 1$

Thus,

Public key is $(\boldsymbol{e}, \boldsymbol{n}) \rightarrow (\mathbf{7}, \mathbf{33})$
Private key is $(\boldsymbol{d}, \boldsymbol{n}) \rightarrow (\mathbf{3}, \mathbf{33})$

Example 2

Step 1: Choose $p = 101$ and $q = 113$

Step 2: Compute $nn = 101 \times 113 = 11413$

Step 3: $\varphi(n) = (p-1) \times (q-1) = 100 \times 112 = 11200$

Step 4: Select the encryption key $\boldsymbol{e}$, such that, $1 < e < \varphi(n)$, $\gcd(e, \varphi(n)) = 1$. Let $\boldsymbol{e} = 3533$

Step 5: Compute $\boldsymbol{d}$, such that $(\boldsymbol{d} \times \boldsymbol{e})\ \boldsymbol{mod}\ \boldsymbol{\varphi}(\boldsymbol{n}) = \mathbf{1}$.
$\boldsymbol{d}$ can be 6597, since $(3533 \times 6597) mod\ 11200 = 1$

Thus,

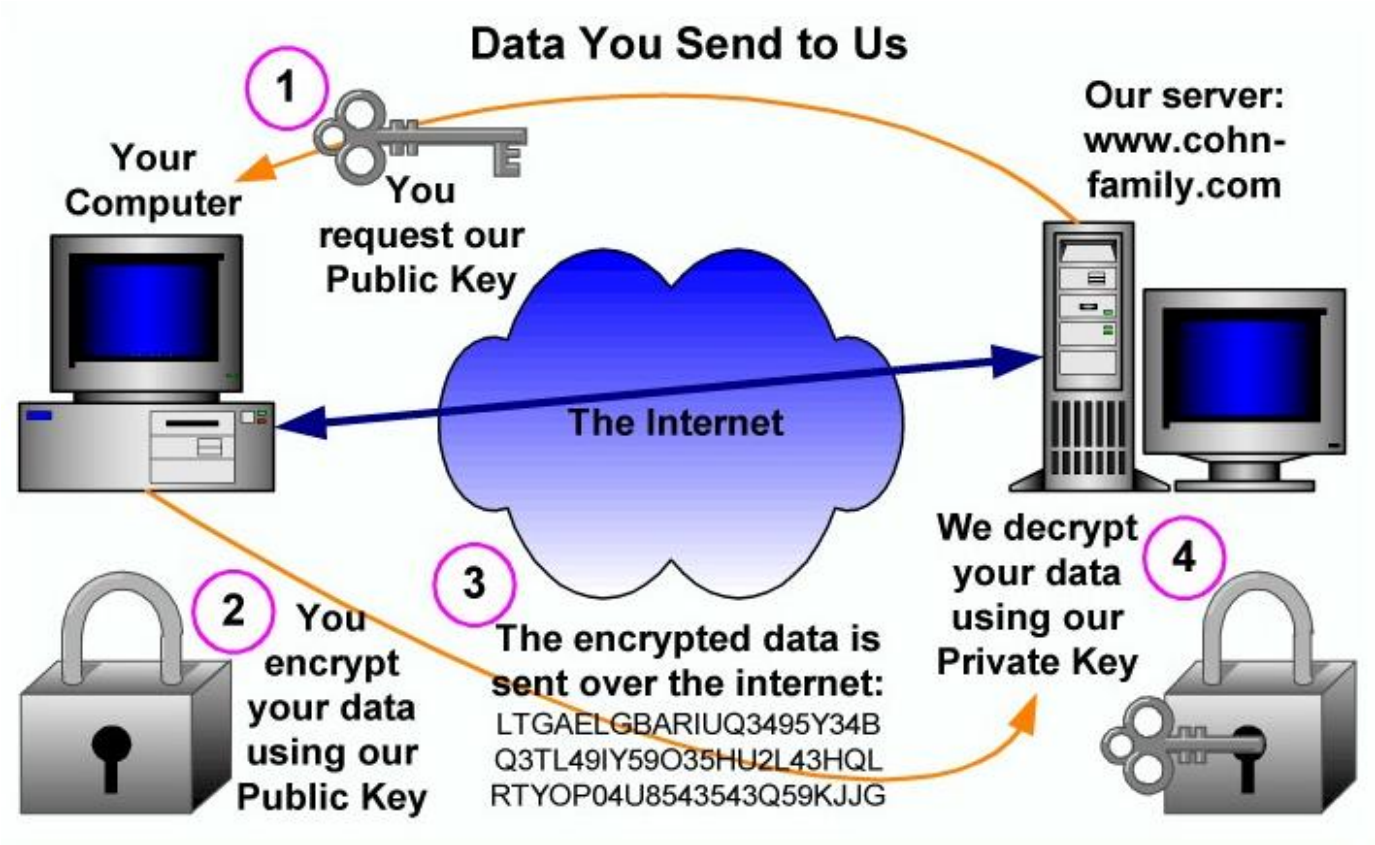
Public key is $(\boldsymbol{e}, \boldsymbol{n}) \rightarrow (\mathbf{3533}, \mathbf{11413})$
Private key is $(\boldsymbol{d}, \boldsymbol{n}) \rightarrow (\mathbf{6597}, \mathbf{11413})$

Today's Homework is:

1. For any two prime numbers (less than 100) not considered in the tutorial, select suitable primes for p and q and using the steps listed above, show how RSA will work (using steps 1-5).
2. Try task 1 for primes above 100.

Tutorial 5

Encryption in modern science- RSA part II



Today's Key Question(s)

- Encryption and decryption using RSA generated keys

What is the Purpose of Tutorial 5?

- To round-up RSA encryption by showing practical implementation.

Stage 2 & 3: Encryption and decryption

Example 1

If Bob wants to send a message to Alice or vice versa, Bob will do so with the public key pair (7,33) and even if the message is intercepted, it is hard to decrypt except the private key pair (3,33) is known. Alice receives the message and decrypts using her private key (3,33).

Assume Bob wants to send the message M to Alice, the process is shown below:-

Encryption: Let M=2, $c = 2^7\ mod\ (33) = 29$
Decryption: $m = 29^3\ mod(33) = 2$

We get the plaintext message $M = 2$ after decryption.

Example 2

Using $(\boldsymbol{e}, \boldsymbol{n}) \rightarrow (\mathbf{3533}, \mathbf{11413})$ and $(\boldsymbol{d}, \boldsymbol{n}) \rightarrow (\mathbf{6597}, \mathbf{11413})$ from example 2 in previous chapter we have that,

Encryption: $c = 2^{3533} mod(11413) = 8620$

Decryption: $c = 8620^{6597} mod(11413) = 2$

Final assignment

1. We have considered the Caesar cipher which falls in the category of mono-alphabetic substitutions. The example we considered was basic using the 25 letters of the alphabet (A-Z). The task below is a slightly modified Caesar cipher (an alphabet with 62 characters was used).

Tasks

a) Lower and upper cases of the English letter (A-Z, a-z) is used together with **something else** to get 62 characters for all possibilities. Figure out what else this could be to add up to 62.

b) Next decrypt the message given below.

```
Xlmw irgvCtxih qiwweki wlepp gpevmjC lsA RSX xs irgvCtx e
qiwweki xsheC! Izir mj mx Aew wyjjmgmirx efsyx 6444 Cievw
eks, sv xs fi qsvi tvigmwi mr xli Ciev 88 FG, rsAeheCw mx mw
rsx. XsheC iegl ws-geppih Wgvmtx Omhhmi Asyph fi efpi xs kix
wirwmxmzi mrjsvqexmsr, mj xliC Aivi irgvCtxih xlmw AeC.
```

NOTE: The plaintext is English and you have to get all upper and lower case right to get credits for this challenge. Try all possibilities.

2. Consider the plaintext

PARLIAMENT HILL

And assume that the letters of the alphabet are numbered as shown:-

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Do the following: -

a) Encrypt the plaintext using RSA choosing two primes above 20 but less than 100 to get ciphertext.
b) Decrypt to confirm ciphertext is correct

The Deadline is: 28th February 2017

Tutorial 6
Feedback

What is the Purpose of Tutorial 6?

- Reflect on skills learned on the programme with a view to encouraging resilience
- Receive feedback on final assignment

What are the key questions?

- What strengths have I demonstrated in my work and what areas of development are there left for me to address?
- What steps do I need to take to improve my academic output?

Activity 1 – Marking your own

Using the mark scheme, identify three things you did well and three things you could improve.

What went well?

1.

2.

3.

What could be improved?

1.

2.

3.

Activity 2 – Responding to feedback

Read through your feedback sheet and highlight on your assignment where you received positive feedback (one colour) and areas for improvement (different colour). You might find it helpful to annotate this with a brief comment or two.

Activity 3 – Looking Forwards: Think, Pair Share

1. Think about how you can use this feedback in your future school work.
2. Talk to your partner about how you both plan to make changes to your school work in the future as result of this feedback
3. Share your ideas as a group.

Referencing correctly

When you get to university, you will need to include references in the assignments that you write, so we would like you to start getting into the habit of referencing in your Brilliant Club assignment. This is really important, because it will help you to avoid plagiarism. Plagiarism is when you take someone else's work or ideas and pass them off as your own. Whether plagiarism is deliberate or accidental, the consequences can be severe. In order to avoid losing marks in your final assignment, or even failing, you must be careful to reference your sources correctly.

What is a reference?

A reference is just a note in your assignment which says if you have referred to or been influenced by another source such as book, website or article. For example, if you use the internet to research a particular subject, and you want to include a specific piece of information from this website, you will need to reference it.

Why should I reference?

Referencing is important in your work for the following reasons:

- It gives credit to the authors of any sources you have referred to or been influenced by.
- It supports the arguments you make in your assignments.
- It demonstrates the variety of sources you have used.
- It helps to prevent you losing marks, or failing, due to plagiarism.

When should I use a reference?

You should use a reference when you:

- Quote directly from another source.
- Summarise or rephrase another piece of work.
- Include a specific statistic or fact from a source.

How do I reference?

There are a number of different ways of referencing, and these often vary depending on what subject you are studying. The most important to thing is to be consistent. This means that you need to stick to the same system throughout your whole assignment. Here is a basic system of referencing that you can use, which consists of the following two parts:

A marker in your assignment: After you have used a reference in your assignment (you have read something and included it in your work as a quote, or re-written it your own words) you should mark this is in your text with a number, e.g. [1]. The next time you use a reference you should use the next number, e.g. [2].

Bibliography: This is just a list of the references you have used in your assignment. In the bibliography, you list your references by the numbers you have used, and include as much information as you have about the reference. The list below gives what should be included for different sources.

Websites – Author (if possible), title of the web page, website address, [date you accessed it, in square brackets].

E.g. Dan Snow, 'How did so many soldiers survive the trenches?', http://www.bbc.co.uk/guides/z3kgjxs#zg2dtfr [11 July 2014].

Books – Author, date published, title of book (in italics), pages where the information came from.

E.g. S. Dubner and S. Levitt, (2006) *Freakonomics*, 7-9.

Articles – Author, 'title of the article' (with quotation marks), *where the article comes from* (newspaper, journal etc.), date of the article.

E.g. Maev Kennedy, 'The lights to go out across the UK to mark First World War's centenary', *Guardian*, 10 July 2014.

University Applications Guidance

For course choices and careers information:	www.brightknowledge.org.uk
For information and statistics on universities and course:	www.unistats.direct.gov.uk
For comprehensive information on universities, including rankings:	www.thecompleteuniversityguide.co.uk

PLEASE NOTE – The Researchers in Schools programme is designed to support the university applications process at your school. The work you complete for the programme should add to your schoolwork rather than detract from it. Please be aware of deadlines and try to manage your workload appropriately. If you are worried about the programme interfering with your schoolwork then please speak to your teacher.

Subject specific resources

https://www.mysterytwisterc3.org/en/

http://www.furthermaths.org.uk/students

http://www.mathscareers.org.uk/