

---

University Of Portsmouth  
BSc (Hons) Computer Science  
First Year

**Core Computing Concepts**

M30220

September 2022 - May 2023

20 Credits

Thomas Boxall  
up2108121@myport.ac.uk

---

# Contents

<b>I</b>	<b>Video Essay</b>	<b>2</b>
<b>1</b>	<b>Introduction To Module</b>	<b>3</b>
<b>2</b>	<b>Reviewing Previous Work</b>	<b>4</b>
<b>II</b>	<b>Web</b>	<b>5</b>
<b>3</b>	<b>Introduction &amp; Markup</b>	<b>6</b>
<b>4</b>	<b>Style</b>	<b>8</b>
<b>5</b>	<b>URLs and Images</b>	<b>9</b>
<b>III</b>	<b>Security</b>	<b>10</b>
<b>6</b>	<b>LECTURE: Week 0 &amp; Introduction</b>	<b>11</b>
<b>7</b>	<b>WEEK 1: Security 101</b>	<b>12</b>
<b>8</b>	<b>WEEK 2: Access Control</b>	<b>17</b>
<b>9</b>	<b>WEEK 3: Cryptography</b>	<b>21</b>

**Item I**

**Video Essay**

# Page 1

## Introduction To Module

📅 27-09-22

🕒 13:00

🎓 Nadim

📍 RB LT1

This module is split into four items. The first of these is a video coursework project. The second, third and fourth are combined into an end of year exam. Each item is worth 25% of the overall module grade, therefore the end of year exam is worth 75%.

This module was created because the University doesn't do modules which are smaller than 20 credits and none of the items are big enough to be their own module.

To pass the module, you need to score at least 40% overall, not in each individual item.

The four items are taught by different lecturers and are shown below

1. Video coursework
2. Web
3. Security
4. Either UXD or DB (which we do is decided for us)

Each item will be introduced to us when we start that item.

### Item 1: Coursework

This is due at 11pm on 16th December 2022. It is to be uploaded to YouTube, with a link to the video put in a PDF document which is uploaded to Moodle.

This item is able to be done either in groups or by individuals, it should be very easy to get a good grade in it.

The task is to select a conversation and analyse the conversation, using supporting research and references.

The video should be at most 4 minutes long, it can be a mixture of different takes edited together. There are a number of different pieces of editing software available on App-Somewhere.

#### More Information

More information for this coursework can be found on a Google Doc which is linked from the Moodle page. This Google Doc links to the official University Coursework information document, the conversations and outlines the lecture plan for the first half of TB1.

There is a one lecture per week and an optional drop in session per week. The drop in sessions are primarily there to answer quick questions.

## Page 2

# Reviewing Previous Work

📅 04-10-22

🕒 13:00

🎓 Nadim

📍 RB LT1

Historically, one of the biggest weaknesses to previous coursework submissions was the lack of knowledge of how it was graded.

For an animated video, look at Powtoons.

You are able to use AI voice generators to speak the script, however this is a risk as its not your voice on your submission. If you do use an AI voice, you must submit the script as a PDF to prove it is your own work.

The following list are things which were included in examples that I think are the attributes of high scoring videos

- Present the video as an argument, with one side then respond to it from the other perspective;
- Lift quotes out of the conversations and question, elaborate and research around them;
- Use evidence for all points

Th argument analysis included after each conversation is new for this year and the use of it won't loose or gain marks. It is there to give guidance for those who are unsure of where to start otherwise.

**Item II**

**Web**

## Page 3

# Introduction & Markup

📅 08-11-22

🕒 13:00

🎓 Rich and Co.

📍 RB LT1

## Introduction to Item II

There are a number of different lecturers on this module: Rich, Matt and Kirsten. The exam will be computer based however not all computer marked. It will comprise mostly of multiple choice questions which will test knowledge of modern HTML and CSS. The multiple choice answers will be evil. The best practice is preparation. Exam date and time will be in January and will be announced on timetable at some point.

There is a Google Doc linked from Moodle which contains all the information and resources about this item. This document contains, pre session, during session and post session work.

There are drop ins on Thursdays in the FTC, these are compulsory.

There is a channel on the Discord Server (#ccc-web) where support can be sought.

The recommended book is available electronically through the library. One of the authors, Remy, has delivered guest lectures at the University.

## Online Resources

Look at Mozilla Developer Network, add MDN to the end of any Google query about web development and their resources will come up.

Do not use W3Schools. It is bad.

## Markup

Markup comes from the days of editors hand writing articles to be printed then annotating that with styles. This document then goes to a Typesetter who would design the content based off of the editors markings, hence markup.

HyperText Markup Language (HTML) is a form of markup, which is non-linear. It is a series of opening and closing tags, which together make an element. Elements can have attributes which provide more information on them or the way in which they should behave.

## HTML Introduction

HTML5, the latest and most up to date version, should always start with the line `<!doctype html>`. This will tell the browser that the page is to be rendered as a HTML5 document.

A HTML document is comprised of two sections, a `<head>` and a `<body>`. In HTML5, the two sections do not need to be marked out as different sections, once you have specified that the document is HTML5 then the renderer is able to infer the difference.

**<head>**

This contains information about the document. Elements which you might see include `<title>` which defines the title of the page and `<meta>` which provides additional information about the webpage. Nothing in the head element is rendered.

**<body>**

This contains the content of the page. Numerous different tags are available within this to define the style of the content.

**Markup**

There are two types of Markup.

**Procedural**

This defines what to do and how it looks. It does not define why to do it.

**Descriptive**

This says what it means, not how it looks or what to do.

This is stratified (separates content from presentation), dynamic (different presentation to suit circumstances) and semantic (enables machine processing).

This means that we use descriptive markup, with semantic value, improving information quality and consequently styling of our pages must be achieved outside HTML.



## Page 4

# Style

📅 15-11-22

🕒 13:00

🎓 Rich & Co

📍 RB LT1

## Cascading Style Sheets

Cascading Style Sheets (CSS) have been around since about 1997. They are a W3C standard for styling HTML and take the form of text files. The files contain rules which users define.

CSS is comprised of a number of rules.

```
LANGUAGE: CSS
1 p{
2   background: red;
3   color: white;
4   padding: 1em;
5 }
```

The rule above will turn the background colour to red, the text colour to white and give a padding on all sides of 1em to every p element in the page.

## Selectors

There are a number of different ways in which we can define what elements in a HTML document we want to target with a given CSS rule.

- `p{}` will target all p elements within the document. This is the same for any other element when the rule is written this way.
- `*{}` will target *everything* in that HTML document.
- `#myid{}` will target the elements with the id of `myid`. This is the same for any other ids used in the same way.
- `.myclass{}` will target all the elements with the class of `myclass`. This is the same for any other classes used in the same way.
- `classOne, classTwo` will target both `classOne` and `classTwo`. This is useful for when multiple components on a HTML page need styling in the same way.

## Page 5

# URLs and Images

📅 22-11-22

🕒 13:00

🎓 Matt & Co

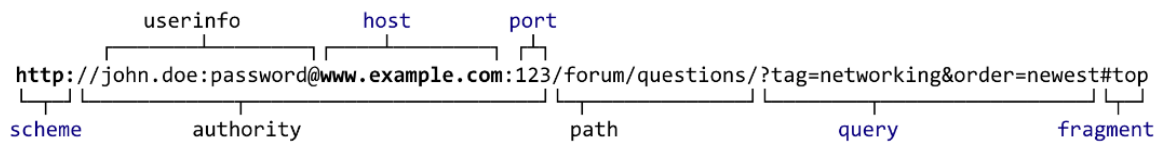
📍 RB LT1

Uniform Resource Locators (URLs), a subset of Uniform Resource Indicators (URIs) allow us to navigate throughout the internet. They take the following form:

`https://port.ac.uk/`

`http://www.example.com/forum/questions/?tag=networking&order=newest#top`

They can be typed into an address bar, hyperlinked or used as the `src` attribute on elements.




URL Structure


**Item III**

**Security**

## Page 6

# LECTURE: Week 0 & Introduction

 24-01-23

 13:00

 David

 RB LT1

This sub-module will use Flipped Learning. There are a collection of videos on Moodle which we will need to watch each week. Lectures will be used to review previous weeks content and metrics based off of quiz scores. The quizzes do not feed into our final grade and can be found on Moodle. Also on Moodle, is a 'hotspots' activity which provides additional information which is needed to complete the quiz.

The lectures will be adapted each week to allow review and consolidation of content.

## Page 7

# WEEK 1: Security 101

📅 25-01-23

👁 Flipped Learning Lecture

### Information Security

The preservation of confidentiality, integrity and availability of information

### Confidentiality

The property that information is not disclosed to unauthorised individuals, entities or processes.

### Integrity

The property of safeguarding the accuracy and completeness of assets.

### Availability

The property of being accessible and usable upon demand by an authorised entity.

Often when introducing systems which protect one of these characteristics, for example confidentiality, there is a trade off that another characteristic will lessen, for example integrity.

### Assets

Anything that has value to the organisation, its business operations and its continuity.

### Threat

A potential cause of an incident that may result in harm to a system or organisation.

Threats can be both internal (employee leaking confidential data) and external (criminal accessing data for financial gain).

### Vulnerability

A weakness of an asset; group of assets; or information system that can be exploited by one or more threats.

### Impact

The result of an information security incident, caused by a threat, which affects assets.

Impacts can include the monetary loss incurred directly due to the loss of information; cost of responding to the incident; fines incurred for failing to adequately and reasonably failing to prevent such an incident; or to the brand or reputation of the brand which ultimately leads to loss of customers.

### Risk

The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

Investment in security isn't like other investments within an organisation as the investments are made to prevent loss of income as a result of an incident where other investments may be made to increase income. The decision to invest in security is often made when weighing up: the cost of dealing with a small security incident frequently versus the cost of dealing with one big security incident which will probably never happen but if it did then it would be catastrophic for the organisation. The process organisations go through to identify, assess and control risks is called *risk management*.

## Assets

Information assets are typically among the highest value assets of an organisation. ISO 27005 defines primary and supporting assets. Where supporting assets are only of interest when assessing information security risks where compromises to the supporting assets may adversely impact the primary assets.

Primary assets	Secondary Assets
Business processes & Activities	Hardware
Information	Software
	Network
	Personnel
	Site
	Organisation's Structure

## Information

Information assets are typically of the highest value to the organisation, this is especially the case for *business critical information* without which the business would cease to operate. This is also the case of *personal information*, which is the data of employees and customers which by law must be adequately protected. *Strategic Information* should be protected, as releasing this information may lose that business a competitive advantage. *High-cost information* is information whose gathering, storage, processing and transmission require a long time and/or involve a high acquisition cost, the impact of losing this information may be that the high costs will be duplicated.

## Business Processes

These are processes that contain secret processes; processes involving proprietary technology; processes that if modified can greatly affect the accomplishment of the organi-

sation's mission; or processes that are necessary for the organisation to comply with contractual, legal or regulatory requirements.

Significant adverse impacts can arise from the failure to adequately document or protect those business processes. Organisations will commonly find out when an employee is off sick, on holiday or leaves the company that the processes they oversaw are not sufficiently documented.

## Hardware

This is the physical technology that: houses and executes the software; stores and carries the data; or provides the interface for data entry/ removal from the system. This includes, but is not limited to: desktops, servers, laptops, scanners, keyboards, monitors and hard drives.

Physical security is just as important as physical access can often mean information can be readily extracted. Whilst the hardware may be relatively cheap, the information stored, processed or captured on it may be worth millions.

## Software

Software, within the information security sphere, comprises of applications, operating systems, assorted command utilities. Software is arguably the most difficult information security component to secure as software development is often under resourced therefore information security is often only added as an afterthought rather than being embedded as an integral part. When designing the specification for new software, the security requirements should be included up-front, at the same time as core functionality. The exploitation of software errors in software programming accounts for a substantial proportion of attacks on information.

## Networks

Distributed hardware and software components are connected through networks by routers, switches, relays, firewalls, etc. Collectively these manage the effective transmission of information between interconnected computing devices. Connections from within the network out onto the internet and to other partner networks, expose systems to attacks. Policies, as well as architectural and technical responses can be put in place to reduce the likely hood of these attacks succeeding. This can be done by examining ports, protocols and packets at the network perimeter to ensure that only the data which is required to support the business to function is being exchanged. Firewalls should be used to create a 'buffer zone' between the internal business network and outside untrusted networks (including the internet). Firewalls should be configured such that everything is denied by default and a white list is implemented which only allows the traffic through which is required. Inbound and outbound data at the perimeter should also be scanned for malicious content.

As well as protecting the perimeter, its also important to protect the internal network. Part of this is ensuring there is no direct routing between internal and external services. Network traffic should be monitored to detect (and then be able to react to) attempted or actual network attacks. Critical business systems should be segregated within the network and appropriate controls should be put in place to access these. Appropriate access controls to both wireless access points and to other hardware should be secure and *should not* be left as default passwords. Network intrusion, prevention and detection tools should be deployed on the network and configured by qualified staff. Systems should automatically generate alerts which staff can manage as part of an incident response plan.

## Personnel

Personnel is an often over-looked component of securing an information system. They themselves are susceptible to numerous vulnerabilities. People make mistakes on a daily basis that compromise information assets. They are also susceptible to social engineering, bribery and blackmail. Due to this, it's important that all staff are adequately trained in how to perform their duties securely. Users have a critical role to play in their organisations security.

Systematic delivery of training should be deployed to ensure employees are trained and to help to enforce a security conscious culture. Organisations should develop a comprehensive set of policies covering security and computer use topics, these policies should be written using plain business terms and reduce the use of technical jargon. New employees should be made aware of policies and the companies procedures as part of their induction. The effectiveness and awareness of training should be monitored. The organisation should strive to promote a security conscious culture where staff feel empowered to voice their concerns. Organisations should also be aware that mistakes will be made by even the most security conscious of individuals.

## Subject or Object

Object of the attack is the entity which is being attacked, the target.

Subject of the attack is the entity carrying out the attack against the target.

Subject attacks the object.

Computers can be compromised which can lead to it carrying out an attack on another machine. A person might be blackmailed or bribed to carry out an attack. In both of these examples, the entity (computer/ person) is both the subject and object of an attack.

## Information Security Governance

### Information Security Governance

How organisations control, direct & communicate their cyber risk management activities.

This will include a collection of policies, including but not limited to: overarching information security policy; ICT acceptable use policy; and other issue specific policies eg remote working. These policies must be continually reviewed and revised to keep up to date with the business needs and continually changing threats/ vulnerabilities.

To remain viable, the security policies must state: the individual responsible for the policy; schedule of review; method of making recommendations for reviews; specific policy issuance and revision dates.

### Policy

A principle or rule to guide decisions and achieve rational outcomes. Should be broadly applicable to the widest possible set of circumstances and contexts supporting employees in deciding the most appropriate course of action in any given situation.

### Procedures

A list of steps that constitute instructions for performing some action or accomplishing some task. These cannot exhaust all possible actions undertaken by an employee.



## Standards

Detailed statements, quantifying what must be done to comply with policy. For example, 'passwords must contain a mixture of 8 numbers, letters and special characters and they should be changed if compromised'. Compliance with standards is also mandatory, they should state what should be done and how it should be achieved.

## Guidelines

A set of recommended actions to assist in complying with policy.

## Disseminating Policies

Policies should be promoted/ supported by a security education, training and awareness (SETA) programme that helps employees do their jobs securely.

Not everyone in the organisation needs a formal degree or certification in information security, however some roles may require certain employees to hold information security academic qualifications or industry certification.

Everyone in an organisation needs to be trained in information security. Training provides employees with hands on instruction with regards to their specific jobs which enables them to perform their duties securely. Management of information security can be developed in-house or outsourced to outside training providers. Training will often make use of safer environments rather than the production systems.

Security awareness is not intended to teach something new. Instead it aims to keep elements of information security at the forefront of employees minds, this is information which they already possess due to their education and training. Materials may be disseminated in a variety of creative means, such as posters, mouse mats or even coffee mugs.

## NCSC Guidance

Good security governance should clearly link security activities to your organisation's goals and priorities; identify the individuals at all levels who are responsible for making security decisions & empower them to do so; ensure accountability for decisions; ensure that feedback is provided to decision-makers on the impact of their choices; and fit into an organisation's wider approach to governance. Security needs to be considered alongside other business priorities such as health and safety or financial governance.

## Incidents Happen

Incidents will happen, we may be able to considerably reduce the likelihood of an incident, however not remove it completely, we can further reduce the risk by minimising the impact of the incident. This is done through incident response management.

## Page 8

# WEEK 2: Access Control

📅 2023-02-01

👁 Flipped Learning Lecture

## Identification & Authentication

Users must be instructed to enable user-specific access controls and given individual accountability for their actions.

Claimed identities must be authenticated. This is the first line of defence for the system and safeguards against unauthorised use (internal and external). Traditional passwords are the most common means of authentication in digital systems, they are conceptually simple for designers & users, and can provide good protection if used correctly; however the protection they provide is often compromised by users.

## Passwords

Passwords have a number of vulnerabilities: it is easy to badly select one; they get written down; infrequently or never changed; same password used for multiple systems; only require them at the start of a session; they can be forgotten; and they can be shared. The traditional defence against password guessing (lock the user out after three failed password attempts) enables a form of Denial of Service (whereby the attacker disrupts availability by deliberately locking out users).

## NCSC Password Guidance

The National Centre for Cyber Security encourage organisations' to reduce reliance on users recall of large numbers of complex passwords. They have published 6 tips.

1. Reduce your organisations reliance on passwords
2. Implement technical solutions
3. Protect all passwords
4. Help users cope with password overload
5. Help users to generate better passwords
6. Use training to support key messages

## Access Control

### Identity

The properties of an individual or resource that can be used to identify uniquely one individual or resource that can be used to identify uniquely one individual or resource.

**Authentication**

Ensuring that the identity of a subject or resource is the one claimed.

**Authorisation**

The process of checking the authentication of an individual or resource to establish their authorised use of, or access to information or other assets.

**Accounting**

Ensures that user activities can be tracked back to them.

**Audit**

Formal or informal review of actions, processes, policies and procedures.

**Compliance**

Working in accordance with the actions, processes, policies and procedures laid down necessarily having independent reviews.

## Authentication

### Factors of Authentication

There are three widely used authentication mechanisms (factors).

**Something a supplicant knows** which includes: personal identification numbers (PIN); passwords; passphrases; and security questions/ answers.

**Something a supplicant has** which includes: dumb cards (magnetic stripe ID cards and ATM cards); smart cards (chip and pin cards); and security token (key fob, card reader etc.)

**Something a supplicant is** which includes: fingerprint; palmprint; retina/iris scanner; voice; keyboard kinetic measurements.

### Strong Authentication

Strong customer authentication is a procedure based on the use of two or more of the following elements - categorised as knowledge, ownership and inherence: something only the supplicant knows; something only the supplicant possesses; and something the supplicant is. In addition, the elements must be mutually independent (which means breach of one doesn't compromise the other).

## Biometrics

Biometric technologies are evaluated on three basic criteria.

**False Rejection Rate (FRR)** is the percentage of identification instances in which authorised users are denied access. This is a Type I error.

**False Accept Rate (FAR)** is the percentage of identification instances in which unauthorised users are allowed access. This is a Type II error.

**Crossover Error Rate (CER)** is the level at which the number of false rejections equals the false acceptances. This is the Equal Error Rate (EER).

## Biometric System Requirements

There are a number of requirements which biometric systems have.

**Universality** - every individual in the population should possess the trait.

**Distinctiveness** - the ability of the trait to sufficiently differentiate between any two persons.

**Persistence** - the trait shouldn't change too much over time on the individual in question.

**Collectability** - the trait should be easy to collect or be measurable.

**Performance** - within a variety of operational and environmental conditions, high recognition accuracy and speed should be achievable.

**Acceptability** - the biometric identifier should have a wide public acceptance and the device used for measurement should be harmless.

**Circumvention** - it should be difficult to spoof the characteristic using fraudulent methods.

## Access Control

Access privileges are specified and subjects' access to objects are determined through a security policy. There are a number of different access control policies.

**Discretionary Access Control** Policy (DAC) - controls access based on identity.

**Mandatory Access Control** Policy (MAC) - controls access based upon security labels.

**Role-Based Access Control** Policy (RBAC) - controls access based on roles.

**Attribute-Based Access Control** Policy (ABAC) - controls access based on attributes.

## File System Permissions

By default, file systems come with four permissions: read, write, execute, and none of the above.

## Privileged Access

The conventional name for the user with top-level access is system or application administrator (sysadmin for short). They can: enrol new users; modify user access right; remove user access rights. They can also modify groups or levels of privilege, rebuild the system, erase data, grant or deny access to applications; change passwords; and even alter or destroy event logging or auditing data.

These accounts have great power and wide-ranging capabilities and their use must be tightly controlled and safeguarded. Their power to disrupt operations, accidental or otherwise is enormous.

## Security Policies

Access privileges are specified and subjects' access to objects are determined through a security policy. There are a number of different access control policies.

### Discretionary Access Control (DAC)

This controls access based on identity. It is at the discretion of the owner and the permissions are often shown as a matrix.

Alternatively an Access Control List (ACL) can be used. These store the access rights to an object within the list.

Alternatively to either of the above, a Capability List (CL or C-List) can be used to store access rights. These store all the access to the rights to an object within a subjects unique list.

### **Mandatory Access Control (MAC)**

This controls access based upon security labels. There is less individual in this as the OS has overall control. Rules are used for defining how the subject can behave. It uses sensitivity (or security) labels to define access rights (these may include: top secret; secret; classified; and unclassified).

MAC makes use of a number of access control models.

**Dell-LaPadula Confidentiality Model** which provides a "no read up no write down" system. This enables users to read everything below them, write to their level of security and have no access to anything above them.

**Biba Integrity model** which provides a "no write up, no read down" system.

**Clark-Wilson Integrity Model** which has a number of rules: no changes by unauthorised subjects; and no unauthorised changes by authorised subjects. Maintenance of internal consistency (system does what is expected without exception) and external consistency (data in the system is consistent with similar data in outside world) is important here.

**Graham-Denning Access Control Model** has three key parts: objects, subjects and rights.

**Brewer-Nash Model** in which subjects can only access one of two conflicting sets of data (which prevents conflicts of interest).

### **Role Based Access Control (RBAC)**

This policy is newer than DAC and MAC. It is a centrally administered set of controls through which permissions are assigned based on roles. Users who perform a similar function are grouped together (for example Moodle has student access and lecturer access). It is a useful model for companies with high employee turnover.

Each user can be a member of many roles and each role can have many users as members. A permission can be assigned to many roles. Each role can have many permissions.

### **Attribute Based Access Control (ABAC)**

This generalises access control based on the role attribute of users. It uses various other attributes of the users including their environment and information assets to determine permissions.

## Page 9

# WEEK 3: Cryptography

📅 2023-02-08

👁 Flipped Learning Slides

Cryptography is a way of turning *plaintext* (the text to be encrypted) into *ciphertext* (an unreadable version that can later be turned back into plaintext).

Encrypting something links four elements together: the plaintext  $m$ ; the ciphertext  $c$ ; the key  $k$ ; and the algorithm  $E$ .

$$c = E_k(m)$$

Modern cryptographic algorithms abide by the following principles

- Large enough key space to resist exhaustive search
- Resistant to frequency analysis
- Small change in plaintext results in large change in ciphertext
- Security depends only on secrecy of key and not on secrecy of algorithm (Kerckhoff's principle)

## Cryptographic Algorithms

### Symmetric

Encryption and Decryption both use the same "secret key". This means the encryption methods can be extremely efficient, requiring minimal processing. Both the sender and receiver must possess the encryption key; and if either copy of the key is compromised, and intermediate can decrypt and read messages.

### Asymmetric

Asymmetric encryption uses two different, but related, keys to encrypt/ decrypt messages. This works as follows: if key A encrypts the message, only key B can decrypt. This methodology has the highest value when one key serves as the private key and the other serves as the public key. It is typically used to encrypt a symmetric session key rather than the plaintext message(s).

## Caesar Cipher

The Caesar Cipher is one of the simplest forms of a cryptographic algorithm. In it, a 'wheel of letters' are turned and letters simply substituted, for example A becomes B, B becomes C and so on.

This cipher can be very easily brute forced as there is a maximum of 25 possible options to try, and using common letter (E T A) frequency, a good guess can be made relatively quickly.

## Symmetric Cryptosystem

A symmetric cryptosystem starts with the plaintext being encrypted with the shared key. This produces the ciphertext which is transmitted to the recipient. The recipient is then able to decrypt the ciphertext using the shared key which produces plaintext.

Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES) are all examples of Symmetric Encryption.

With symmetric encryption, the primary challenge is distribution of keys. In general we will need  $n \times (n - 1)/2$  keys where  $n$  is the number of parties who want to communicate.

## Diffie-Hellman Key Exchange

The Diffie-Hellman (DH) key exchange uses asymmetric encryption to exchange session keys, these are limited use symmetric keys for temporary communication. This allows two entities to conduct, quick efficient, secure communication based on symmetric encryption which is more efficient than asymmetric encryption for sending message.

DH based key establishment is incorporated into a number of standard protocols: TLS/SSL and IPSec. DH based key establishment is also used in a variety of applications: GlobalProtect VPN; and WhatsApp.

## Asymmetric Cryptosystem

An asymmetric cryptosystem works by the symmetric encryption key being used to encrypt the plaintext. This is then transmitted to the recipient where it is held until the encryption key is received. The encryption key (which has already been used to encrypt the plaintext) is passed through an encryption algorithm that uses the recipient's public key. This, now encrypted, message is transmitted to the recipient where they can use their private key to decrypt it. The recipient now has the symmetric encryption key and can use that to decrypt the ciphertext they received into the plaintext.

RSA and Elliptic Curves are examples of Asymmetric Encryption.

## RSA

RSA is the most famous asymmetric cryptographic algorithm, developed by Rivest, Shamir and Adleman in 1978. It is based on number-theoretical properties of natural numbers.

The steps below show RSA in a nutshell.

1. Choose two large primes  $p$  and  $q$ , and calculate  $n = p \times q$
2. From  $n$  follow some maths steps to calculate the value  $e$  and  $d$
3. Publish  $n$  and  $e$ , keep  $d$  a secret and destroy  $p$  and  $q$
4. Encryption of  $m$  is now  $c = m^e \pmod n$
5. Decryption of  $c$  is then  $m = c^d \pmod n$

## Example encryption and decryption

Shown below is an example encryption of the plaintext GAGA

1. Encode the letters as ASCII numbers 71 65 71 65
2. Encrypt each letter in turn using  $c = m^e \pmod n$  assuming  $e = 131$  and  $n = 232$ . ( $d = 11$  but this is only known to the receiver).

3. This gives  $71^{131} \pmod{323} = 10$  and  $65^{131} \pmod{323} = 126$ .

4. The message that gets transmitted is 10 126 10 126.

Shown below is the decryption of the message encrypted above.

1. The receiver knows  $d = 11$  and  $n = 323$  and the algorithm  $m = c^d \pmod{n}$

2.  $10^{11} \pmod{323} = 71$  and  $126^{11} \pmod{323} = 65$

3. Convert 71 and 65 to letters using ASCII

4. Results in G and A

The examples shown here use very small primes to make the calculations easy. In reality, the prime numbers used are much bigger.