Section 7 Lecture 42 – P.A.I.N.

Many transactions nowadays are carried out over the internet – what is known as *e-commerce*.

Purchasing goods, for example, over the internet comes with specific difficulties and problems that we need to address to ensure the transaction is exactly as it should be – payment is made and the goods are received by the correct person.

There are really four issues to consider – these are often known by the acronym PAIN.

Privacy

Privacy (also termed *secrecy* or *confidentiality*) is the first of these categories.

Essentially, any sensitive information sent during the transaction should be kept secure from other parties. This would include things like personal information and payment information (such as credit card numbers) which are sent via the internet when making a transaction, and is vital they are kept safe and secure – you don't want a hacker to be able to obtain any details about you!

This is where encryption is particularly important!

Authentication

The second category is *authentication*.

How can you be certain that the person you are communicating with is actually who they say they are? When buying goods over the internet, this works for both parties – the buyer wants assurance that the website they are dealing with is actually a genuine company and not some scam. Similarly, the company wants to be sure that the person placing the order is who they say they are.

This is also important for, say, the credit card companies – they want to be sure that the card is being used by its rightful owner and not through identity theft, say – this is especially important for credit card companies as they are liable for fraudulent transactions!

In a shop, this "authentication" might be done via a signature ("something unique") or a PIN number ("something known") but how do you do something similar over the internet? We will look at this when we discuss *digital signatures* shortly.

Integrity

The third of our categories is *integrity*.

When data is passed over a network, and when it is stored in an organisation's database, there is a danger that the data might be altered (either deliberately or accidentally).

We have looked in the coding part of the course about techniques to help with accidental errors here – errors can be detected and corrected with an appropriate coding system.

Deliberate errors are harder to deal with – we need some mechanism to ensure that the data can't be deliberately changed (for example, sending a bank withdrawal request for £100 and having it changed to £1000000 during transmission)

Both coding and cryptography clearly have an important role to play here.

Non-repudiation

The final category is *non-repudiation*.

This refers to the assurance that no party involved in a legitimate transaction can later deny that the transaction was legitimate, or actually took place.

For example, you should not be able to go onto a gambling site, lose thousands of pounds, and then the next day claim you didn't do it (or vice versa, win thousands of pounds and have the site claim you never placed the bets).

Digital signatures are going to be important here – we will discuss shortly.

Summary

All of these issues are important. In an ideal system we will have all of them – during the next few lectures we will look at how we can achieve this through a *public-key infrastructure*.