Dashboard / My classes / CS808 / Week 3 (w/c 7th October): Further Cryptography / 3.2 Article: Introducing Public Key Cryptography NH

CS808: Computer Security Fundamentals

3.2 Article: Introducing Public Key Cryptography

✓ **Done:** View

In this article we will look at the use of public key encryption as a solution for the key distribution problem. Recall that the key distribution problem is the issue of trying to agree a shared key over an insecure channel. One solution to this is to make use of key exchange algorithms such as Diffie-Hellman. Alternatively, we can use public key cryptography, sometimes known as asymmetric cryptography.

In this approach we generate a key pair for each entity (such as an individual) who wishes to communicate securely. There is a private key, which is kept only by the entity, and the public key which can be shared without compromising security. This key pair is mathematically linked in such a way that data encrypted with the private key can only be decrypted by its corresponding public key and vice versa. It is also computationally infeasible to derive the private key from the public key and vice versa.

In order to communicate securely with Bob, we would need to encrypt using Bob's public key. Only Bob will then be able to decrypt this, as Bob is the only person with access to the corresponding private key.

You can also provide some confidence in authenticity through public key cryptography. For example, if Bob wishes to share information with Alice and provide Alice assurance it comes from Bob then Bob should encrypt the message using his private key. This will not provide confidentiality, but the public key for Bob is the only key which can decrypt this. Thus, if Alice can successfully decrypt using the public key for Bob then there is some assurance the message has come from Bob. In practical use, there are further steps to ensure the integrity of the message which we will come back to elsewhere. Clearly if Bob's private key was compromised this would be problematic. However this demonstrates how public key cryptography can be used to provide non-repudiation.

It is also useful to note that we can achieve confidentiality and authenticity by layering of encryption. In the message above which is encrypted with Bob's private key for authenticity, it could then be encrypted once more with Alice's public key to ensure only Alice is able to decrypt it. Once Alice removes the outer layer of encryption, Alice can decrypt once more using Bob's public key for assurance that the message came from Bob.

There are a few things to highlight about public and private key pairs. Whilst the natural assumption is that an entity would have only one public and private key pair, the reality is that there may be multiple key pairs for a single entity. Some of these key pairs may also be ephemeral, that is they are for temporary use e.g. for a single communication session over the internet. As a real world example, the popular messaging app Signal makes use of multiple key pairs.

Another point to note is that sometimes keys may be compromised (e.g. if stored on a server which is compromised) or otherwise lost. In such a situation, the entity who owns the key pair needs to revoke their public key and generate a new key pair.

Hopefully this brief overview gives you an insight into the general structure of public key cryptography. In the upcoming steps we will see how this is applied in practice.

Last modified: Thursday, 8 September 2022, 11:17 AM

◄ 3.1: Video: Diffie-Hellman Key Exchange (09:15)

Jump to...

3.3: Video: RSA (10:12) ►