“Modern Cryptography – A Mathematician in Cyberspace”
Dr Richard Price
GCHQ

Cryptography is at the heart of some of GCHQ’s main objectives namely the protection of government communication and information systems and support for cyber security.

Cryptography is the science of information security. Its origin is usually dated from about 2000 BC, with the Egyptian practice of hieroglyphics whose full meaning was only known to an elite few. Julius Caesar is believed to be the first to use a simple code. He created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. This form of cryptography required both the sender and receiver to know the key.

However, in today's computer-centric world, cryptography is most often associated with scrambling or encrypting information and its subsequent decryption. It has four main objectives: Privacy/confidentiality i.e. can only be read by the holder of the common key. Integrity i.e. the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected. Authentication i.e. the sender and receiver can confirm their identity and the origin/destination of the information. Non-repudiation i.e. the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

The Internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain. Most if not all of the day-to-day transactions on the Internet involve encryption security systems. Mathematical procedures and computer programs are key to developing safe systems but consideration must be given to the regulation of human behavior and the adoption of hard-to-guess passwords.

It is therefore not surprising that GCHQ employs about 100 mathematicians and has set up research institutions in both Bristol and London. It also funds about 15 post-doctoral projects.

Dr Price gave a brief insight into the future and the possible development of quantum computers capable of solving the current factoring encryption systems. As a result, much of the research is aimed at anticipating what will be needed to maintain the security and integrity of world-wide communications.

Given on Wednesday 6th November 2013 at the Royal Agricultural University