# Computing and the Net / Great idea - hide it

## Britain has often led the world in computing - then lost its edge. Duncan Campbell reveals how GCHQ dismissed the code that drives deals on the internet

**By Duncan Campbell**
**Thursday May 6, 1999**

British government scientists, whose discovery of a new type of secret communications was "the most significant event in the history of cryptography" for more than 500 years, failed to notice the value of their discoveries, a leading cryptographer has revealed. Two American groups repeated the research, published the ideas, and laid the foundations for the information society and electronic commerce.

Dr Whitfield Diffie, the co-inventor of "public key cryptography" told the British Society for the History of Mathematics last week that he accepted claims by Government Communications Headquarters (GCHQ) that members of its staff had been first to set out the principles of public key cryptography. The method is now the basis of most digital security systems.

Diffie, a "distinguished engineer" with Sun Microsystems, California, compared his own work published in 1976 with a recent claim that British government cryptographers had discovered the same ideas over the preceding six years. Diffie's invention, together with later ideas for making it work efficiently, began a revolution in communications. It solved the critical problem of how to send secret messages across open channels (such as radio), without having to share vulnerable codebooks or encryption keys.

But it was not until November 1997 that GCHQ's sister organisation, the Communications-Electronic Security Group (CESG) published a claim on the internet that its staff had got there first. CESG is responsible for the British government's secret codes.

Diffie told an audience of mathematicians and net enthusiasts that he accepted that the CESG papers were probably authentic. He said that he had been tipped off about the claim 20 years earlier. He revealed that in 1982, he had made a private visit to Cheltenham to meet the British inventor, James Ellis who had told him "you did more with it than we did".

Diffie also recounted how GCHQ's top cryptologist, Sean Wylie, visited his counterpart in the US National Security Agency and told him about the discovery, reportedly saying: "Do you see anything to this - we don't."

But within three years, the value of the discovery had become exceedingly obvious. US nuclear weapons scientists used it to provide much higher control over the release of weapons and to verify arms control treaties. Its importance grew with the rise of digital communications.

Diffie's lecture was attended by David Kahn, author of The Codebreakers and the doyen of writers in the field. Kahn described his invention as "the most significant event in the history of cryptography" since the discovery of polyalphabetic substitution cyphers in the 15th century. Even modern systems or the famous wartime Enigma cyphers had only been extensions of that system.

Dr James Ellis, the chief of three British scientists involved, died in 1997. In 1987, he had retired and had written up his discovery. He had been led to believe that this would be published by GCHQ soon afterwards, belatedly making his reputation.

By 1987, according to Diffie, secrecy about the discovery was "completely unnecessary". But GCHQ sat on his work for another 10 years, and Ellis died with his achievements unknown and unrewarded.