organisasi rahasia Inggris, mengungkapkan bahwa kriptografer di GCHQ telah mengantisipasi beberapa pengembangan akademik. Dilaporkan, sekitar tahun 1970, James H. Ellis telah memahami prinsip kriptografi kunci asimetris. Pada tahun 1973, Clifford Cocks menemukan sulisi yang esensialnya menyerupai algoritme RSA. Dan pada tahun 1974, Malcom J. Williamson diklaim telah mengembangkan algoritme pertukaran Diffie-Hellman.

Kriptografi kunci-publik dapat juga digunakan untuk mengimplementasikan skema tanda tangan digital. Tanda tangan digital berhubungan dengan tanda tangan pada umumnya; mereka memiliki karateristik yang sama dimana mudah bagi pengguna untuk membuatnya, tetapi sangat sulit bagi orang lain untuk memalsukannya. Tanda tangan digital dapat juga secara permanen mengikat pada konten pesan yang sedang ditanda tangani; mereka lalu tidak dapat 'dipindahkan' dari satu dokumen ke dokumen yang lain, dan setiap usaha akan dapat terdeteksi. Pada skema tanda tangan digital, terdapat dua algoritme: satu untuk *menandatangani*, di mana kunci rahasia digunakan untuk memproses pesan (atau hash dari pesan, atau keduanya), dan satu untuk *verivikasi,* di mana kunci publik yang sesuai digunakan dengan pesan untuk memeriksa validitas tanda tangan. RSA dan DSA merupakan dua skema tanda tangan digital yang paling terkenal. Tanda tangan digital merupakan pusat dari operasi infrastruktur kunci publik dan banyak skema keamanan jaringan lainnya (seperti Transport Layer Security, VPN, dll).

Algoritme kunci publik paling sering didasari pada teori masalah kompleksitas komputasional, sering dengan teori bilangan. Sebagai contoh, kekuatan RSA berhubungan dengan masalah faktorisasi integer, sedangkan Diffie-Hellman dan