kunci *privat*. Sistem kunci pablik dikonstruksikan sangat baik sehingga kalkulasi dari satu kunci ('kunci privat') secara komputasional tidak mirip dengan (kunci 'publik') walaupun secara kebutuhan mereka mirip. Malah, kedua kunci dihasilkan secara rahasia, sebagai pasangan yang tidak berhubungan. Sejarawan David Kahn menjelaskan kriptografi kunci public sebagai konsep baru paling revolusioner dalam bidang ini sejak substitusi polialfabetik yang ditemukan pada masa Renaissance. Dalam ekosistem kunci-publik, kunci publik dapat secara bebas terdistribusi, saat pasangannya kunci privat harus selalu terjaga rahasia. Pada sistem enkripsi kunci-publik, *kunci publik* digunakan untuk enkripsi, sedang *kunci privat* atau *rahasia* digunakan untuk dekripsi. Sementara Diffie dan Hellman tidak dapat menemukan sistem seperti itu, mereka menunjukkan bahwa kriptografi kunci-publik memang benar mungkin dengan menunjukkan protokol Diffie-Hellman key exchange, sebuah solusi yang sekarang digunakan secara luas dalam komunikasi aman, mengizinkan dua kelompok untuk secara rahasia membagi kunci enkripsi.

Jurnal Diffie dan Hellman menyebar luas pada dunia akademi dalam mencari sistem enkripsi kunci-publik praktis. Lalu pada tahun 1978 Ronald Rivest, Adi Shamir, dan Len Adleman, menemukan solusi yang kini dikenal sebagai algoritme RSA.

Algoritme Diffie-Hellman dan RSA, sebagai tambahan dalam menciptakan contoh algoritme kunci-publik kualitas tinggi pertama yang dikenal publik, telah sangat luas digunakan. Yang lain termasuk Kriptosistem Cramer-Shoup, Enkripsi ElGamal, dan varian Teknik kurva eliptis. Lalu, dokumen yang dipublikasikan pada tahun 1997 oleh *Government Communication Headquarters (GCHQ)*,