untuk peningkatan kekuatan secara signifikan. Sehingga, pada tahun 2012, standar nasional Amerika memilih SHA-3 sebagai standar desain hash yang baru.

Message authentication code (MAC) hampir mirip dengan fungsi hash kriptografi, kecuali terdapat kunci rahasia yang dapat digunakan untuk membuktikan nilai hash melalui serangkaian resep kerumitan tambahan yang melindungi skema serangan algoritme penyingkat sederhana, dan dianggap cukup menguntungkan.

Kriptosistem kunci-simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi sebuah pesan, walaupun pesan atau kelompok pesan dapat memiliki kunci yang berbeda dari yang lain. Kerugian yang paling signifikan dari chiper simetris ialah kebutuhan *manajerial kunci* untuk menggunakannya secara aman. Setiap sepasang pihak komunikasi yang berbeda harus, idealnya, membagi kunci yang berbeda, dan juga membagi textchiper yang berbeda juga. jumlah kunci yang dibutuhkan meningkat dua kali lipat dari jumlah anggota jaringan, yang sangat cepat membutuhkan skema manajemen kunci komplek untuk menjaga semuanya tetap konsisten dan rahasia. Kesulitan dari menciptakan kunci rahasia yang aman di antara dua pihak yang saling berkomunikasi, ialah, ketika belum adanya *jaringan aman* di antara keduanya, juga kehadiran *chicken-and-egg problem* yang dianggap menjadi tantangan praktikal untuk pengguna kriptografi di dunia nyata. (Berkas:Diffie and Hellman.jpg|jmpl|kiri|Whitfield Diffie dan Martin Hellman, penulis jurnal pertama kriptografi kunci-publik) Pada jurnal pionir tahun 1976, Whifiled Diffie dan Martin Hellman mengusulkan istilah dari kriptografi*kunci-publik* (juga, secara umum, disebut *kunci asimetris*) pada dua istilah yang berbeda namun secara matematis terdapat kunci yang berhubungan, yaitu kunci *publik* dan