Satu atau lebih kriptografi sederhana sering digunakan untuk mengembangkan algoritme yang lebih kompleks, disebut sistem kriptografi, atau *kriptosistem*. Kriptosistem (seperti enkripsi ElGamal didesan untuk menyediakan fungsi tertentu (seperti enkripsi kunci publik) sembari menjamin sifat keamanan tertentu keamanan (seperti serangan teks-terpilih) seperti pada model oracle acak. Kriptosistem menggunakan sifat kriptografi sederhana utama untuk mendukung sifat keamanan sistem. Tentu saja, karena perbedaan antara kriptosistem dan kriptografi tidak jelas, kriptosistem yang canggih dapat diperoleh dari kombinasi beberapa kriptosistem sederhana. Pada banyak kasus, struktur kriptosistem melibatkan komunikasi maju mundur di antara dua atau lebih kelompok dalam ruangan. (seperti di antara pengirim dari pesan aman dan penerimanya) atau melewati waktu (seperti data yang dilindungi dengan kriptografi). Kriptosistem yang seperti itu disebut *protokol kriptografi*.

Beberapa kriptosistem yang terkenal termasuk *enkripsi RSA*, tanda tangan Schnorr, enkripsi El-Gamal, PGP, dll. Kriptosistem yang lebih rumit melibatkan sistem uang elektronik, sistem *tanda-tangan enkripsi*, dll. Beberapa kriptosistem *teoritikal* termasuk *sistempembuktian interaktif*, seperti *pembuktian pengetahuan-nol*), sistem untuk *pembagian rahasia*, Hingga saat ini, banyak sifat keamanan kriptosistem didemonstrasikan menggunakan teknik empirial atau menggunakan alasan ad hoc. Saat ini, terdapat upaya untuk mengembangkan teknik formal untuk menyelesaikan keamanan kriptosistem; Hal ini secara umum disebut *keamanan terbukti*. Ide umum dari keamanan terbukti ialah untuk memberikan argumen tentang kesulitan komputasional yang dibutuhkan untuk membahayakan aspek keamanan kriptosistem (dari setiap musuh).