DSA berhubungan dengan masalah logaritma diskrit. Baru-baru saja, *kriptografi kurva eliptis* telah ditemukan, sistem di mana keamanan yang didasari pada masalah teoretis bilangan yang melibatkan kurva eliptis. Dikarenakan kesulitan masalah pokok, kebanyakan algoritme kunci-publik melibatkan operasi seperti eksponensial dan perkalian aritmetika modular, di mana teknik ini secara komputasional lebih *mahal* ketimbang teknik yang digunakan pada banyak chiper blok, khususnya dengan ukuran kunci yang dibutuhkan. Hasilnya, kriptosistem kunci-publik seringnya merupakan *kriptosistem hybrid*, yang merupakan algoritme enkripsi kunci-simetris berkualitas tinggi digunakan untuk pesan itu sendiri, sedang kunci simetris yang relevan dikirimkan dengan pesan, tetapi dienkripsikan menggunakan algoritme kunci publik. Hampir sama, skema tanda tangan hybrid sering digunakan, di mana fungsi hash kriptogfari dihitung secara komputer, dan hanya hash hasil yang ditanda tangani secara digital.

Banyak karya teoritikal kriptografi berkaitan dengan kriptografi sederhana-algoritme dengan sifat kriptografi dasar-dan hubungannya pada masalah kriptografi lainnya. Alat kriptografi yang lebih sulit lalu diciptakan dari kriptografi sederhana ini. Kesederhanaan ini menyediakan sifat yang penting, yang digunakan untuk mengembangkan alat yang lebih kompleks yang disebut *kriptosistem* atau *protokol kriptografi*, yang menjamin sifat keamanan level satu atau lebih tinggi. Bagaimanapun, perbedaan antara kriptografi *sederhana*dan kriptosistem, cukup tipis; sebagai contoh, algoritme RSA kadang disebut kriptosistem, dan kadang sederhana. Contoh tipikal kriptografi sederhana termasuk fungsi pseudorandom, fungsi satu-arah, dll.