

The security of RSA

RSA Labs Challenge : factoring primes set

Key length	Year	Time
140	1999	1 month
155	1999	4 months
160	2003	20 days
200	2005	18 months
768	2009	3 years

Challenges are no longer active

ECC - Elliptic-Curve Cryptography

Key Size	256 or 448 bits
Speed	<ul style="list-style-type: none">~ factor of 10^6 cycles / operation• Key generation: 1 - 5 ms (way faster than RSA)• Encryption: 1 - 5 ms• Decryption: 1 - 5 ms
Mathematical Foundation	Elliptic curves over finite fields