Choose a Method

Lenstra and Verheul Equations (2000)
Lenstra Updated Equations (2004)
ECRYPT II Recommendations (2012)
NIST Recommendations (2012)
ANSSI Recommendations (2010)
Fact Sheet NSA Suite B Cryptography (2013)
Network Working Group RFC3766 (2004)
BSI Recommendations (2014)

Compare all Methods

1 Reference for the comparison

You can enter the year until when your system should be protected and see the corresponding key sizes or you can enter a key/hash/group size and see until when you would be protected.

Enter an elliptic curve key size: � 256 bits

2 Compare

Method	Date	Symmetric	Asymmetric	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
[1] Lenstra / Verheul ❓	2084	135	7813 ⁶⁸¹⁶	241	7813	257	269
[2] Lenstra Updated ❓	2090	128	4440 ⁶⁹⁷⁴	256	4440	256	256
[3] ECRYPT II	2031 - 2040	128	3248	256	3248	256	256
[4] NIST	> 2030	128	3072	256	3072	256	256
[5] ANSSI	> 2020	128	4096	200	4096	256	256
[6] NSA	-	128	-	-	-	256	256
[7] RFC3766 ❓	-	136	3707	272	3707	257	-
[8] BSI (signature only)	> 2020	-	1976	256	2048	250	256