Cryptography formulary

✔ Symmetric algorithms

Name	Key length (bits)	Block size (bits)	Stream parameters	Fast	Noise resistant	Time (years)*	Notes
DES	56 + 8 (parity)	64		No	No		Use XOR,shift and permutation (implemented in hardware)
3DES (2 Keys)	56 (memory ⩾2^59 bits) / 112 (otherwise)	64		No	No		
3DES (3 Keys)	112	64		No	No	<20	
IDEA	~~64~~ 128	64		???	Yes		Good for low spec. devices
RC2	8-1024 (usually 64)	64		Yes (?)	No		
RC4	???	Stream		Yes	No		Security through obscurity
Salsa20	128/256	Stream	Nonce (64 bits) + Counter (64 bits)	Yes	No	>20(128) >>20(256)	20 operations, salsa20/8 and salsa12/12 makes respectively 8 and 12 operations (faster and more insecure)
ChaCha20	128/256	Stream	Nonce (64 bits) + Counter (64 bits)	Yes	No	>20(128) >>>20(256)	20 operations

Name	Key length (bits)	Block size (bits)	Stream parameters	Fast	Noise resistant	Time (years)*	Notes
ChaCha20 IETF	128/256	Stream	Nonce (96 bits) + Counter (32 bits)	Yes	No	>20(128) >>>20(256)	limit of 256 GB
AES	256,192,128	128		Yes (if use 128 bits key with CBC)	Yes (if use CTR, es. AES-128-CTR)	>20(128) >>20(192) >>>20(256)	

* Time is referred to the calculators performances in 2010

✔ Mode of operation

Name	Type	IV	Padding	Notes
ECB	Block	No	Yes	Insecure (Not safe)
CBC	Block	Yes	Yes	
CBC-CTS	Block	Yes	No	Doesn't increase data size, good for disk encryption
CTR	Stream	Nonce+Counter		Ideal for small datas
IGE	Block	Yes	Yes	Used in AEAD

✔ Asymmetric algorithms

Name	Notes
RSA	Based on private and public keys
Diffie-Helman	Based on always new number (public), every connection is different from the one before, (only if Ephemeral)
ECDH	Diffie-Hellman with Elliptic curve (Better)

Name	Notes
ECIES	generates a symmetric key and give information to generate it on the other side

Time (year)*	Key length	Key length (ECC)
<1	1024	160
<20	2048	224
>20	3072	256
>>20	7680	384
>>>20	15360	512

* Time is referred to the calculators performances in 2010

✔ Hash algorithms

Name	Block	Digest	Capacity	Strength Compared to symmetric ones	Time (years)*
MD2	8	128			
MD4	512	128			Insecure
MD5	512	128			Insecure
SHA1	512	160			<1
SHA224 (SHA2)	512	224			<20
SHA256 (SHA2)	512	256			>20
SHA384 (SHA2)	512	384			>>20
SHA512 (SHA2)	512	512			>>>20
SHA224 (SHA3)	1152	224	448	112	<20
SHA256 (SHA3)	1088	256	512	128	>20

Name	Block	Digest	Capacity	Strength Compared to symmetric ones	Time (years)*
SHA384 (SHA3)	832	384	768	192	>>20
SHA512 (SHA3)	576	512	1024	256	>>>20
SHAKE128	1344	variable	256	min(d/2,128)	
SHAKE256	1088	variable	512	min(d/2,256)	

* Time is referred to the calculators performances in 2010

✔ AE mode of operation (AEAD)

Name	Notes
CCM	Slowest one (Use CBC-MAC)
GCM	Most used
OCB	Fastest one
EAX	Slow but small, very good for low resources systems