if(is) internet security.

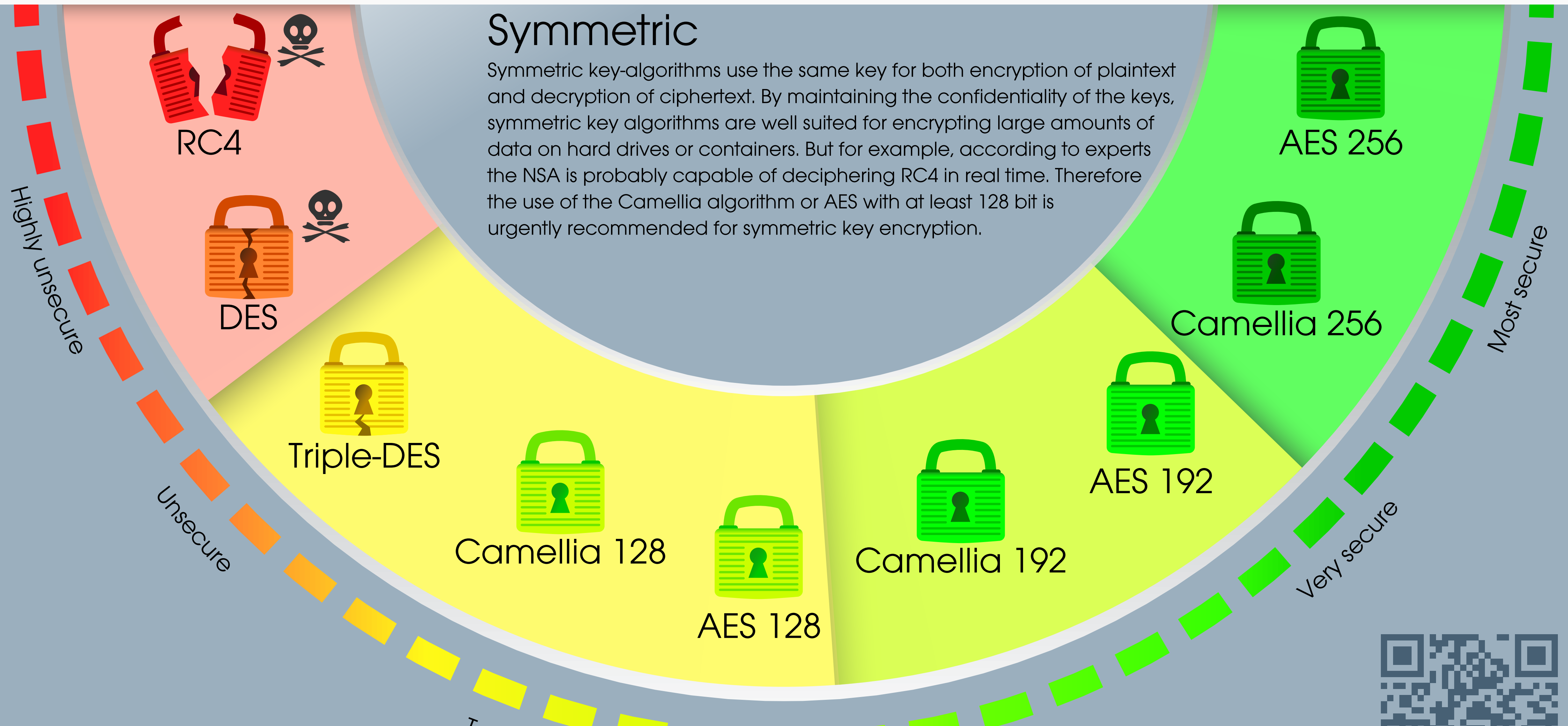
Institute for Internet Security
Cryptographic Algorithms

http://www.if-is.net/crypto-poster/

Status: 2014-05-26
Author: Dominique Petersen
petersen@internet-sicherheit.de
Design: David Bothe
bothe@internet-sicherheit.de

Symmetric

Symmetric key-algorithms use the same key for both encryption of plaintext and decryption of ciphertext. By maintaining the confidentiality of the keys, symmetric key algorithms are well suited for encrypting large amounts of data on hard drives or containers. But for example, according to experts the NSA is probably capable of deciphering RC4 in real time. Therefore the use of the Camellia algorithm or AES with at least 128 bit is urgently recommended for symmetric key encryption.



Highly unsecure

RC4

DES

Unsecure

Triple-DES

Camellia 128

AES 128

Tolerable

Secure

Camellia 192

AES 192

Very secure

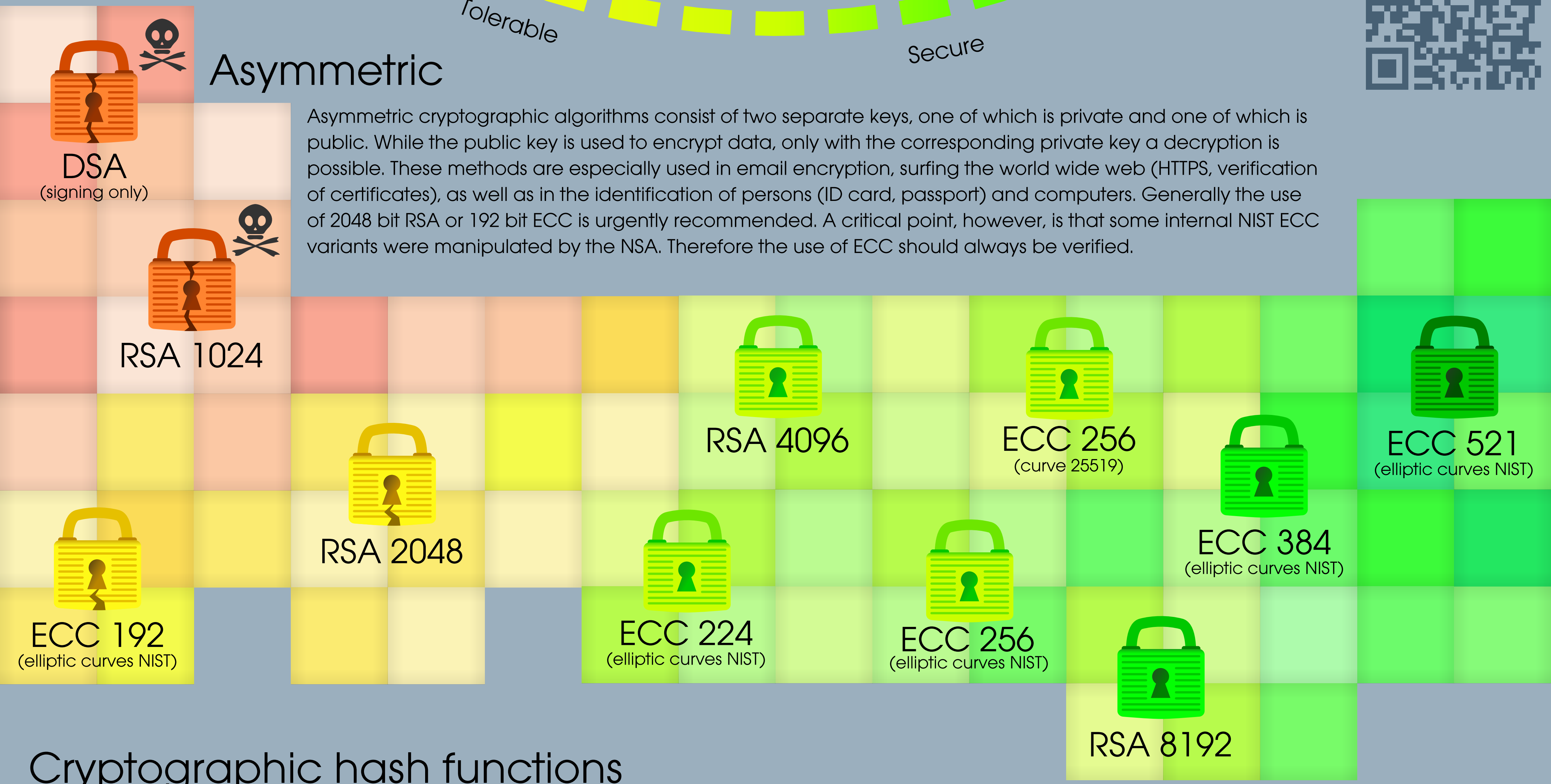
Camellia 256

AES 256

Most secure

Asymmetric

Asymmetric cryptographic algorithms consist of two separate keys, one of which is private and one of which is public. While the public key is used to encrypt data, only with the corresponding private key a decryption is possible. These methods are especially used in email encryption, surfing the world wide web (HTTPS, verification of certificates), as well as in the identification of persons (ID card, passport) and computers. Generally the use of 2048 bit RSA or 192 bit ECC is urgently recommended. A critical point, however, is that some internal NIST ECC variants were manipulated by the NSA. Therefore the use of ECC should always be verified.



DSA
(signing only)

RSA 1024

ECC 192
(elliptic curves NIST)

RSA 2048

ECC 224
(elliptic curves NIST)

RSA 4096

ECC 256
(elliptic curves NIST)

ECC 256
(curve 25519)

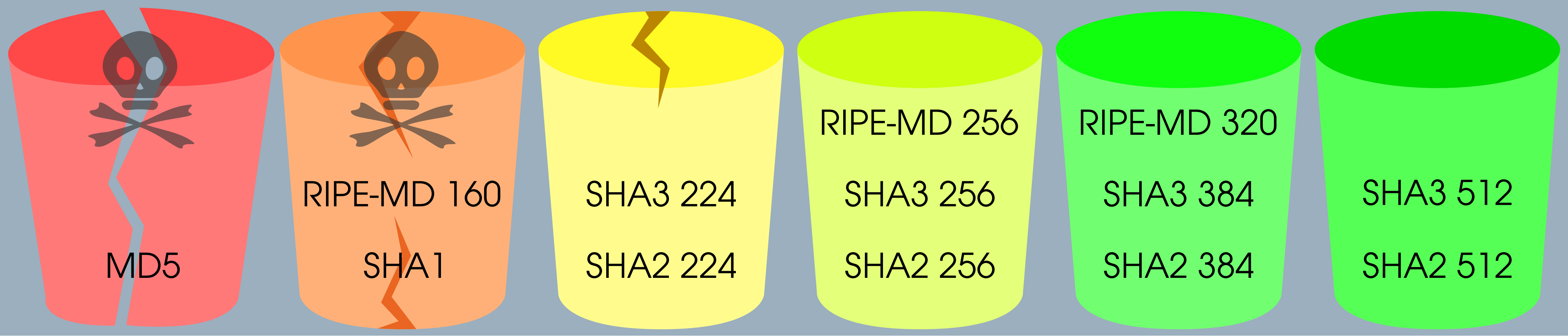
RSA 8192

ECC 384
(elliptic curves NIST)

ECC 521
(elliptic curves NIST)

Cryptographic hash functions

Cryptographic hash functions are used to reduce an arbitrary set of data to a single number of specific length (so-called fingerprint, e.g. 160 bit). Since they are operating one-way only, there are no feasible options to restore the original data. In consequence of their poor performance, asymmetric key algorithms are not suitable for large amounts of data. Hash functions are therefore of central importance. During the process of signing a generated fingerprint of a message by using the public-key method, a verification of the message's origin can be performed and be evaluated whether the message has not been tampered with by a third party. If, however, compromised algorithms, such as MD5, are used, almost any manipulated message can be silently foisted. When using cryptographic hash functions, it is recommended that at least one algorithm of the RIPE-MD-256 or 256 bit SHA2/3 family should be chosen.



MD5

RIPE-MD 160
SHA1

SHA3 224
SHA2 224

RIPE-MD 256
SHA3 256
SHA2 256

RIPE-MD 320
SHA3 384
SHA2 384

SHA3 512
SHA2 512