Basic Cryptography

Kresten Jacobsen

Intro to System Security

Goals

Prevention

Detection

Recovery

C-I-A

Confidentiality

Integrity

Availability

Threats

Snooping

Modification

Spoofing

Repudiation of Origin

Denial of Receipt

Delay

Security Policies

Requirements

- Common understanding (implicit / explicit)
- Trust (in people and computers)
- Assumption (that policies are enforced)

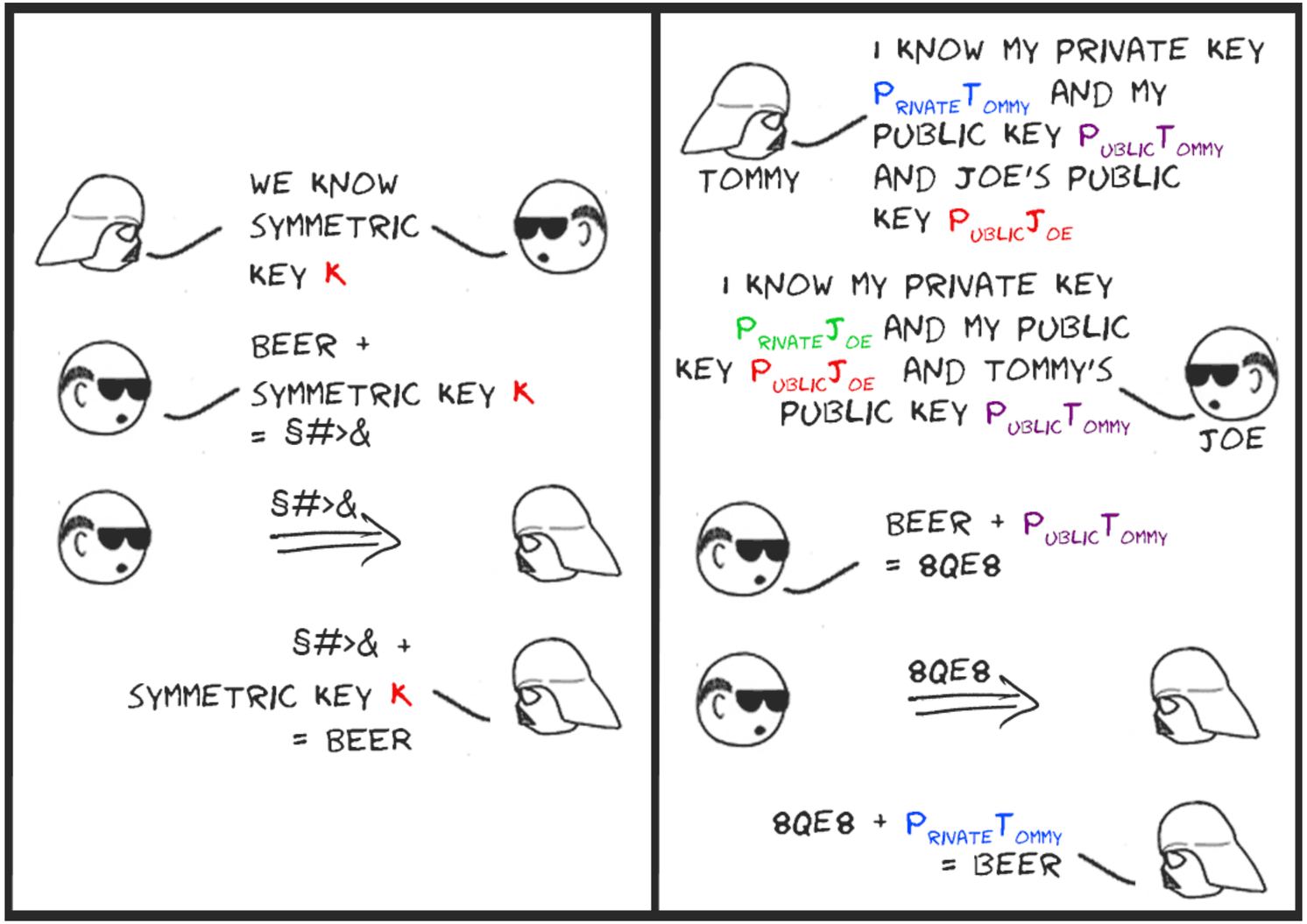
Policy types

- Confidentiality
- Integrity Policy
- Availability Policy

Basic Cryptography - Overview

- Symmetric cryptosystems
  - Transposition ciphers
  - Substitution ciphers
  - Diffie-Hellman key exchange
- Asymmetric Cryptography
  - Private / public key
  - Requires public key infrastructure
- Cryptographic Checksums
- Digital Signatures

Symmetric vs. Asymmetric encryption



Diffie-Hellman simplified

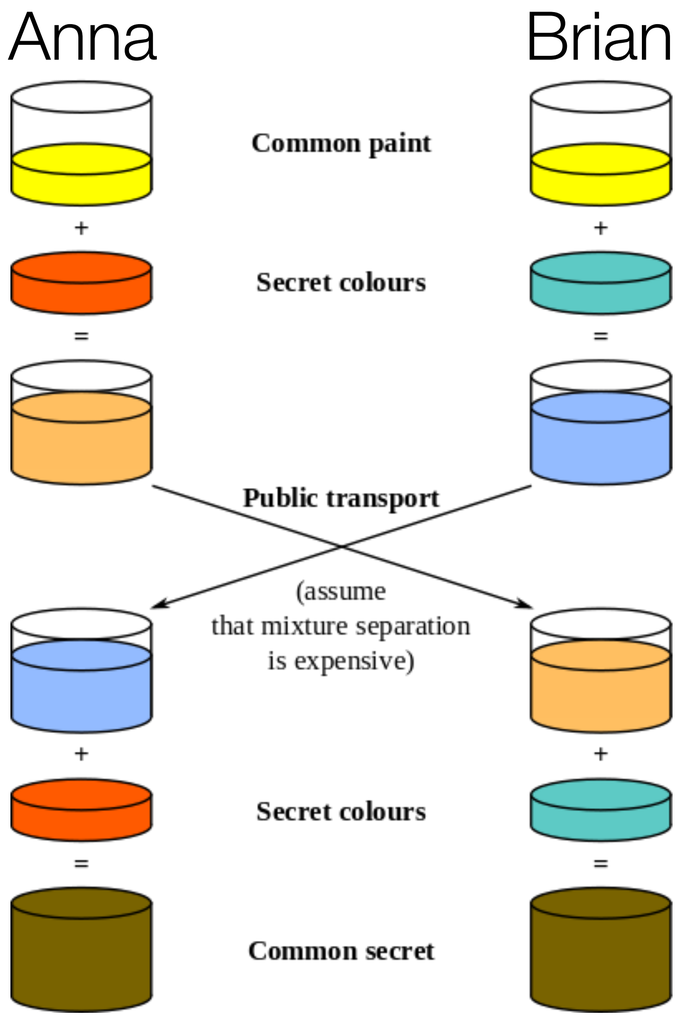
Yellow (Y)
+
red (R)
= orange (Y+R)

Send orange (Y+R)

Receive blue (Y+G)

Mix (Y+G)+R

Y+G+R



Yellow (Y)
+
green (G)
= blue (Y+G)

Send blue (Y+G)

Receive orange (Y+R)

Mix (Y+R)+G

Y+R+G

Cryptographic Checksums

Principles

- Easy to calculate
- Impossible to reverse
- Unlikely to create collisions

Weaknesses

- Guessable (not reversible)
- Possible to create collisions

IT Security Guidelines for Transport Layer Security (TLS)

Versions

Recent versions of TLS are more secure than older versions. The oldest three versions of TLS, SSL 1.0, SSL 2.0 and SSL 3.0 cannot be used securely. The most recent version of TLS, TLS 1.3 offers the best protection.

Version	Status
TLS 1.3	Good (3)
TLS 1.2	
TLS 1.1	Phase out (3)
TLS 1.0	
SSL 3.0	Insufficient (3)
SSL 2.0	
SSL 1.0	

Table 1 – Versions

TLS 1.2	TLS 1.3
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE RSA TLS_AES_256_GCM_SHA384

	Key exchange	Certificate verification	Bulk encryption	Hashing
Good	ECDHE	ECDSA RSA	AES_256_GCM CHACHA20_POLY1305 AES_128_GCM	(HMAC-)SHA-384 (HMAC-)SHA-256
Sufficient	DHE		AES_256_CBC AES_128_CBC	(HMAC-)SHA-1
Phase out	RSA*		3DES-CBC*	
	* Written as TLS_RSA_WITH_...		* Written as 3DES_EDE_CBC or DES_CBC3	

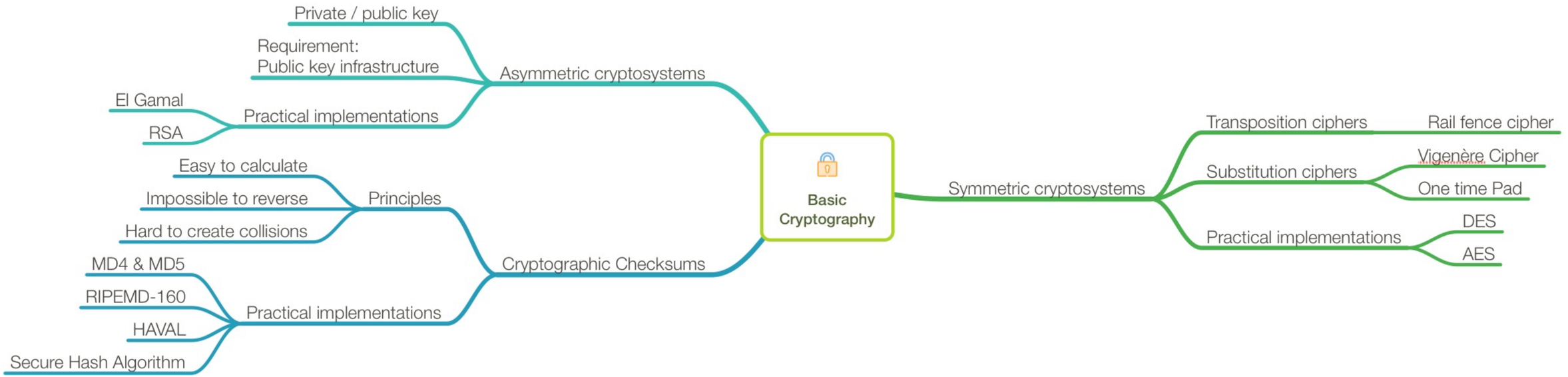
Figure 2 – Cipher suite notation in TLS 1.2 and TLS 1.3. The table summarizes algorithm selections and their security level.
Not included in the (old) cipher suite notation are: versions; hash functions for certificate verification; hash functions for key exchange; key sizes & choice of groups; and options. These can be found in their respective sections. For ordering, refer to the section Prefer faster and safer algorithms.

Algorithm	Status
ECDHE	Good (3)
DHE[26]	Sufficient
RSA	Phase out (2; 3)
DH[25]	Insufficient
ECDH[27]	
KRB5	
NULL	
PSK	
SRP	

Table 4 – Algorithms for key exchange

Algorithm[35, 36]	Status
HMAC-SHA-512	Good (2; 3)
HMAC-SHA-384	
HMAC-SHA-256	
HMAC-SHA-1	Sufficient (3)
HMAC-MD5	Insufficient (2; 3)

Table 7 – Hash functions for bulk encryption and the generation of random numbers


Basic Cryptography
Symmetric cryptosystems
Transposition ciphers
Rail fence cipher
Substitution ciphers
Vigenère Cipher
One time Pad
Practical implementations
DES
AES
Cryptographic Checksums
Asymmetric cryptosystems
Private / public key
Requirement:
Public key infrastructure
Practical implementations
El Gamal
RSA
Principles
Easy to calculate
Impossible to reverse
Hard to create collisions
Practical implementations
MD4 & MD5
RIPEMD-160
HAVAL
Secure Hash Algorithm