02

OPEN ORIENTED

凹 凸 实 验 室

https之加密算法

2017.03.20

相关加密算法

1、散列算法

2、对称加密算法

3、非对称加密算法

1、散列算法

又称 哈希算法(加密)、杂凑算法(加密)、摘要算法、签名算法

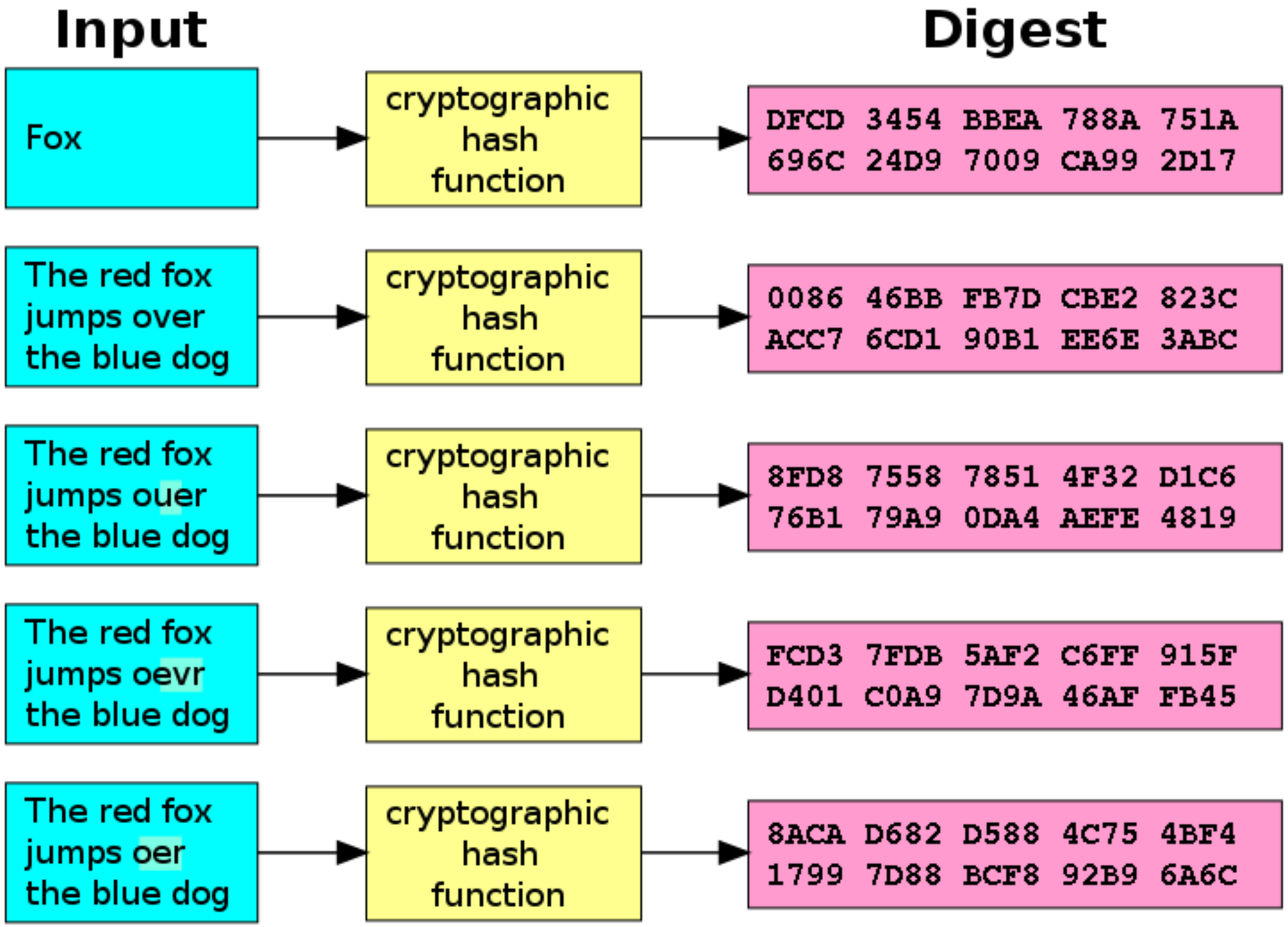
常见的散列算法：MD5、SHA-1、SHA-2 等

1. 通过输入可以容易地计算出输出

2. 很难从给定的输出反推出输入，即不可逆性

3. 不能修改输入（哪怕是微小的修改）而使得输出不变

4. 不能找出2个不同的输入，使得输出一样


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

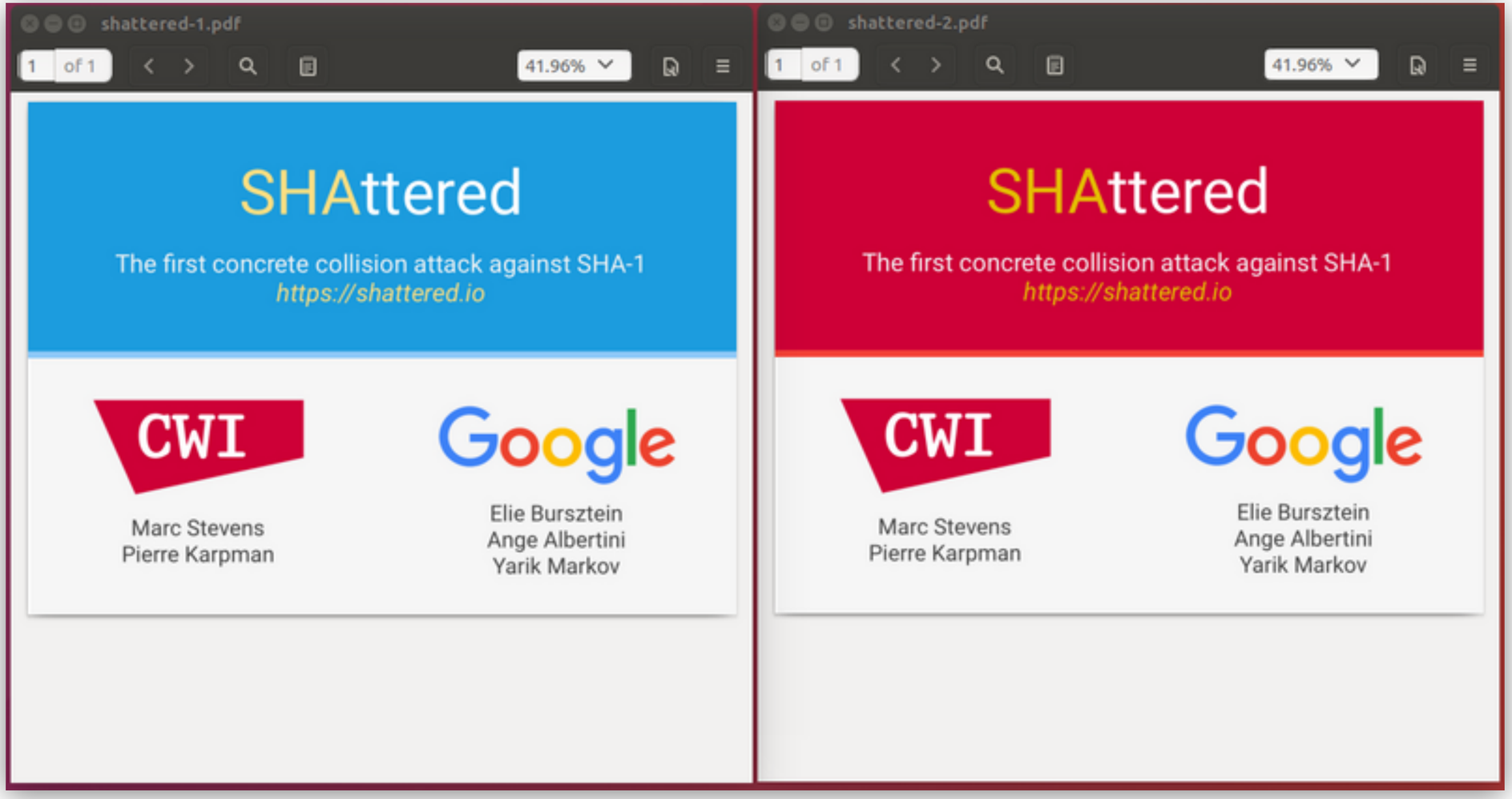
散列算法家族

Comparison of SHA functions [edit]

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Rounds	Operations	Security (bits)	Example Performance[2] (MiB/s)
MD5 (as reference)		128	128 (4 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Or	<64 (collisions found)	335
SHA-0		160	160 (5 × 32)	512	$2^{64} - 1$	80	And, Xor, Rot, Add (mod 2^{32}), Or	<80 (collisions found)	-
SHA-1		160	160 (5 × 32)	512	$2^{64} - 1$	80		<80 (theoretical attack[3] in 2^{61})	192
SHA-2	*SHA-224*	224	256 (8 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112	139
	SHA-256	256						128	
	SHA-384	384	512 (8 × 64)	1024	$2^{128} - 1$	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192	154
	SHA-512	512						256	
	SHA-512/224	224						112	
	SHA-512/256	256						128	
SHA-3	*SHA3-224*	224	1600 (5 × 5 × 64)	1152	∞	24	And, Xor, Rot, Not	112	-
	SHA3-256	256		1088				128	
	SHA3-384	384		832				192	
	SHA3-512	512		576				256	
	SHAKE128	*d* (arbitrary)		1344				min (*d*/2, 128)	-
	SHAKE256	*d* (arbitrary)		1088				min (*d*/2, 256)	

SHAttered事件

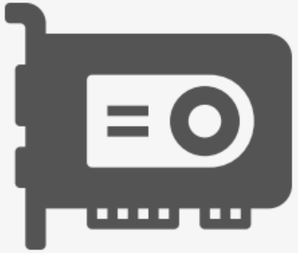
2017年2月23日，CWI和Google的研究人员公开了2个PDF文件，这是2个不同的PDF文档，但是它们的SHA-1校验值是一样的



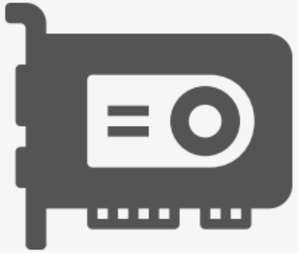
SHAttered 和其他方式对比

Shattered compared to other collision attacks

MD5
1 smartphone
30 sec

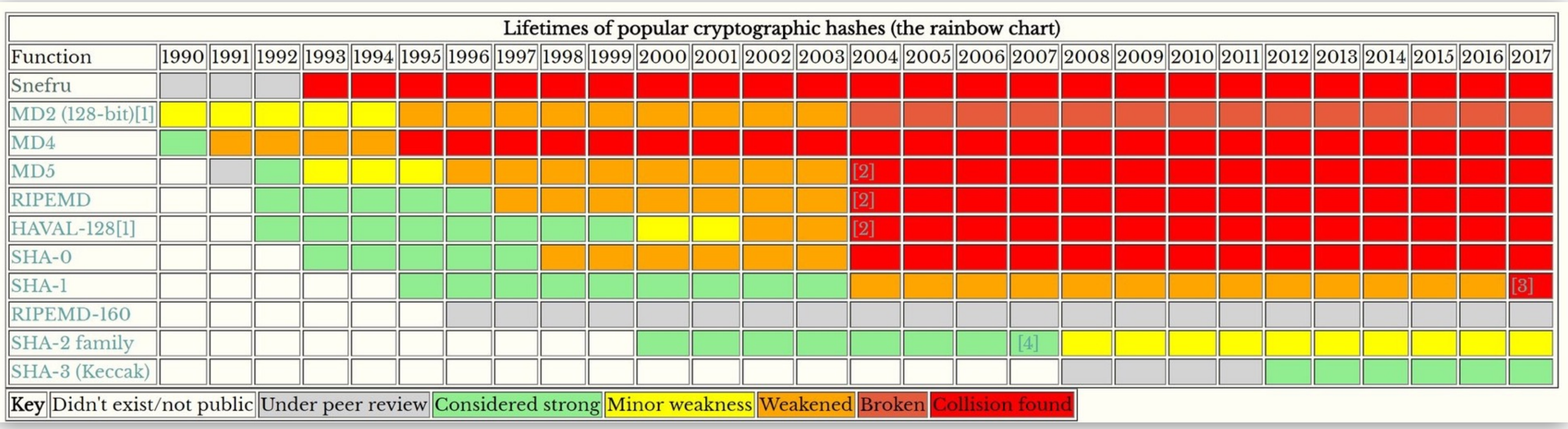


SHA-1 Shattered
110 GPU
1 year



SHA-1 Bruteforce
12,000,000 GPU
1 year

散列算法死亡时间表



Lifetimes of popular cryptographic hashes (the rainbow chart)

Function	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Snefru																												
MD2 (128-bit)[1]																												
MD4																												
MD5															[2]													
RIPEMD															[2]													
HAVAL-128[1]															[2]													
SHA-0																												
SHA-1																												[3]
RIPEMD-160																												
SHA-2 family																		[4]										
SHA-3 (Keccak)																												

Key: Didn't exist/not public | Under peer review | Considered strong | Minor weakness | Weakened | Broken | Collision found

SHA-1 现状

1、对于SSL证书，Windows已于2017年1月1日起停止支持SHA1证书。

2、对于代码签名证书，Windows早在2016年1月1日就停止接受没有时间戳的SHA-1签名的代码和SHA-1证书。

3、Chrome浏览器已经逐步地废弃了SHA-1证书支持，现在最新版的Chrome已经彻底不支持了。

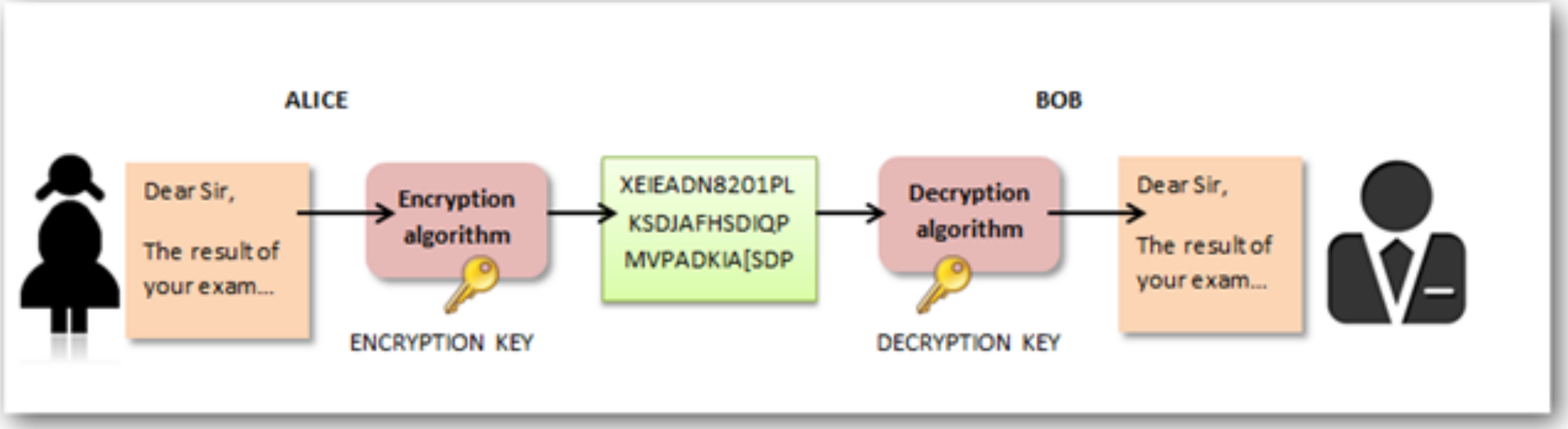
4、Mozilla自2017 年 1 月1 日后不再信任SHA-1证书

2、对称加密

常用的有：DES、3DES、AES、RC2、RC4、RC5和Blowfish

特点：

- 加密解密用的是同一套密钥
- 加密、解密速度较快，可用于大量数据加密



3、非对称加密

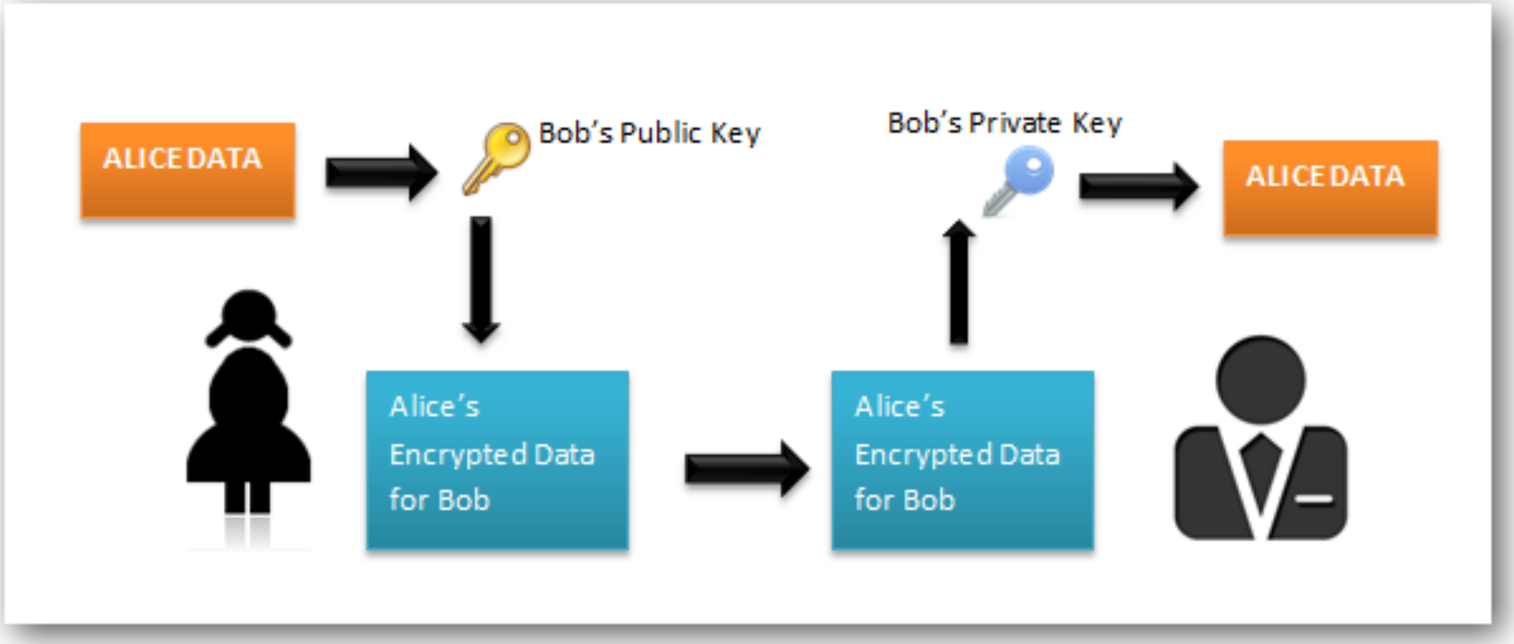
又称公开密钥加密算法

常用的有：RSA、ElGamal、 ECC 椭圆曲线算法

以RSA算法为例，常见的有：

- RSA-768（已被破解）
- RSA-1024（常用，但不推荐）
- RSA-2048（推荐）

非对称加密特点



- 有公钥和密钥，加密解密用的是不同的钥匙；即公钥加密的数据只有私钥才能解密；反之，私钥加密的数据需要公钥才能解密
- 加密、解密速度较慢，用于少量数据加密
- 公钥可以公开传播，私钥需要自己保管
- 加密的数据长度不能大于私钥长度

用openssl加密解密数据

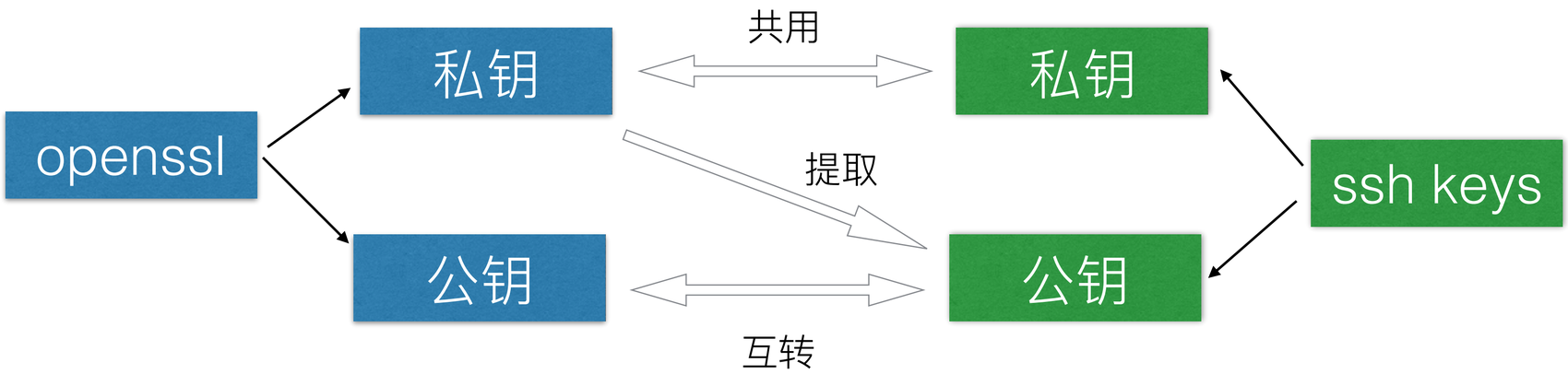

```
openssl genrsa -out private.key 2048      //生成私钥
```

```
openssl rsa -in private.key -pubout -out pub.key    // 从私钥提取公钥
```

```
echo -n "123456" | openssl rsautl -encrypt -inkey pub.key -pubin >encode.result
  //加密数据
```

```
cat encode.result | openssl rsautl -decrypt  -inkey private.key  //解密
```

生成ssh钥匙对： ssh-keygen -t rsa -f testfile -C "for test” //底层是用openssl的库



参考资料

从SHAttered事件谈安全：https://segmentfault.com/a/1190000008496343

shattered事件官网：http://shattered.io/

RSA密钥长度、明文长度和密文长度：http://www.metsky.com/archives/657.html

SSL常见加密算法：http://www.willrey.com/support/ssl_DES.html

openssl生成钥匙对、加密解密数据，http://blog.chinaunix.net/uid-25063573-id-3700746.html

ssh、openssl key之间的转化：http://www.cnblogs.com/pixy/p/4722381.html

THANKS

FOR YOUR WATCHING

02

OPEN ORIENTED

凹 凸 实 验 室