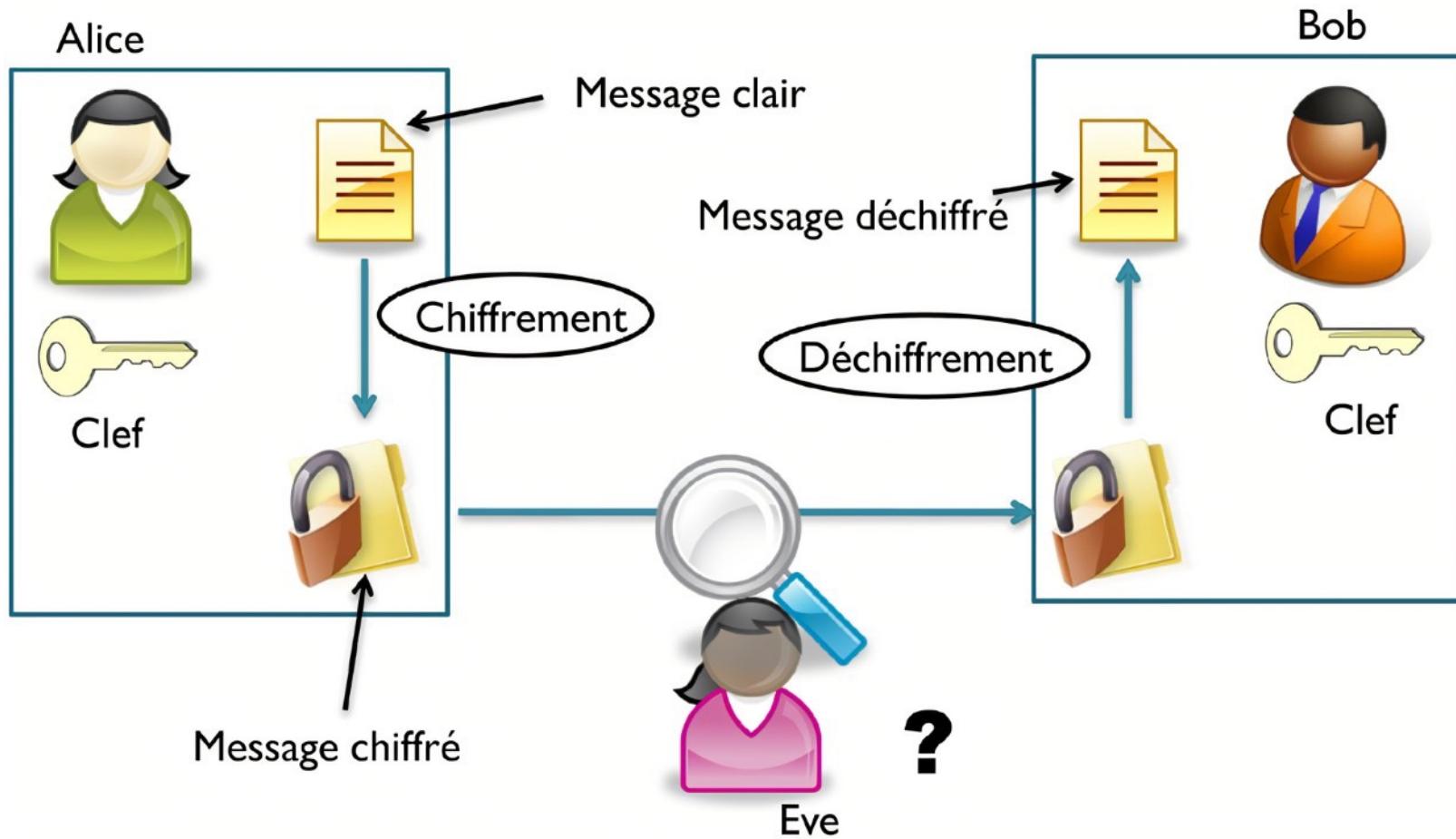


Technologies for E- Commerce

CAN302

**Department of Communications and Networking
Xi'an Jiaotong-Liverpool University (XJTLU)**

Week10 – Https



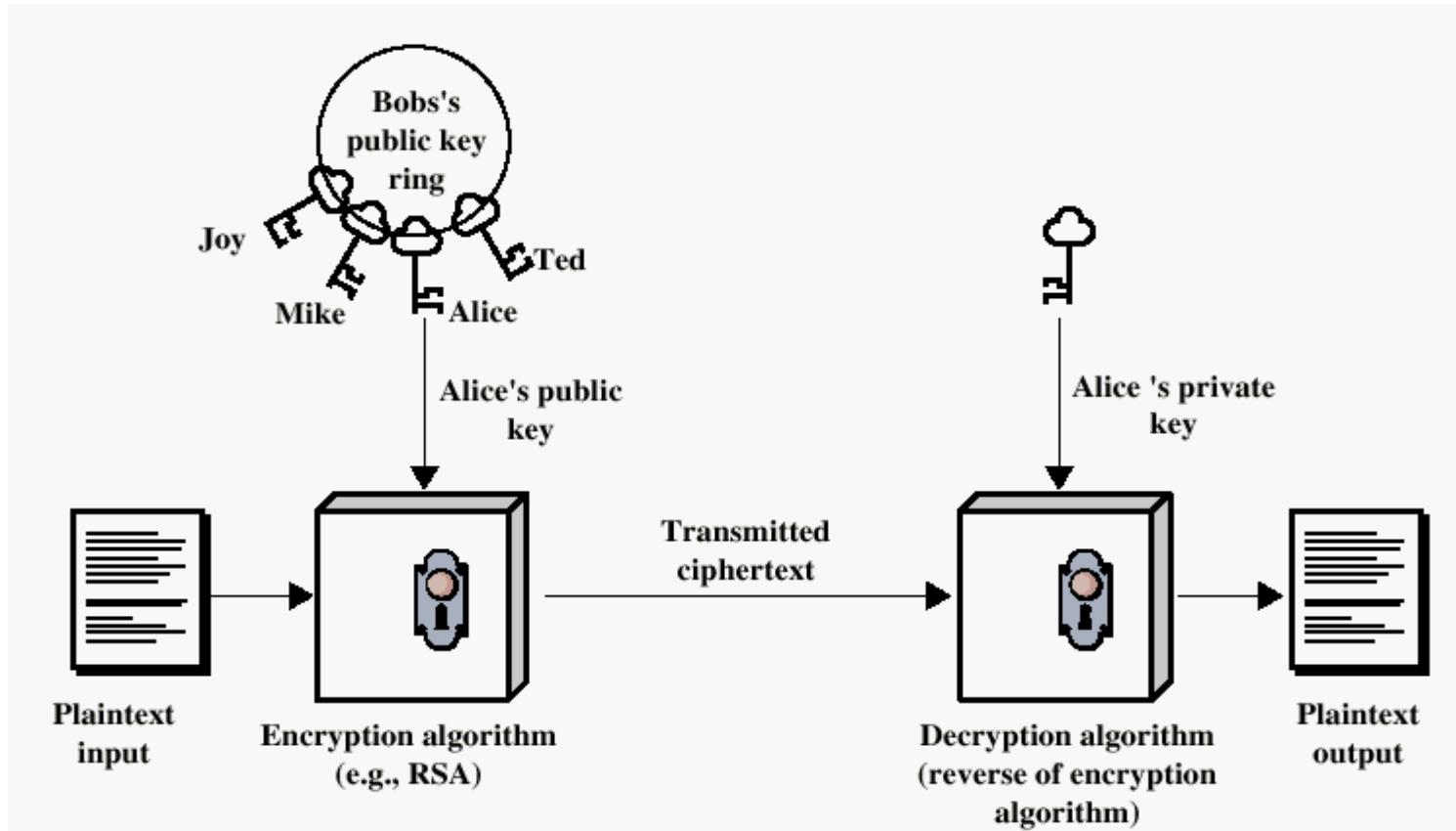
Apply encryption technologies to build a safe channel

Some ideas about https



- Symmetric encryption is quick and safe but difficult to share the key.
- If we can find a way to share the key, we can build a secure channel.
- DH is a safe way to negotiate a key but cannot against middle-man.
- RSA/ECC can share a public key, it is a potential candidate to negotiate the key.

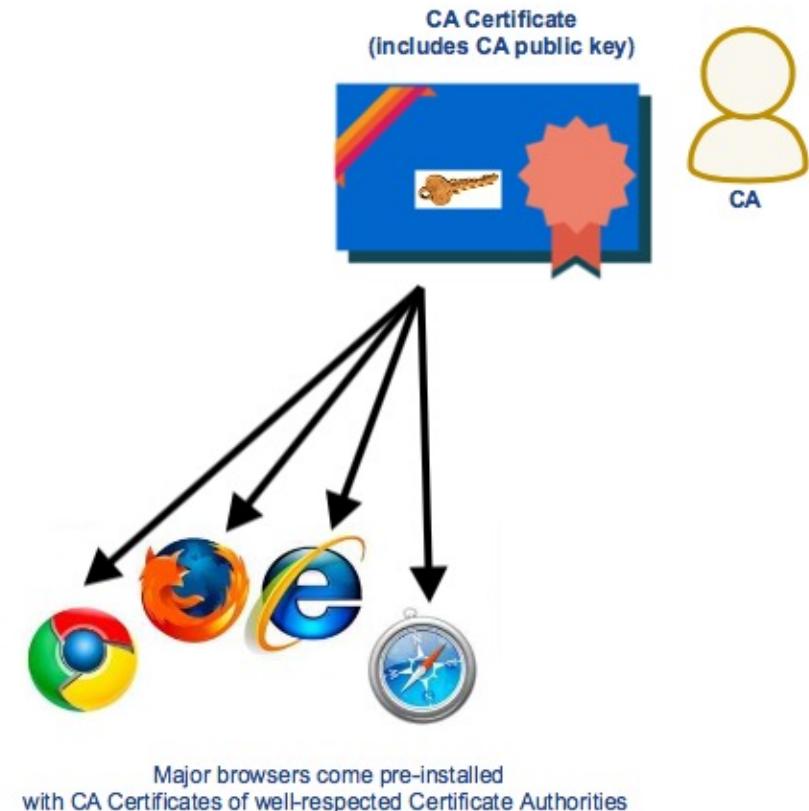
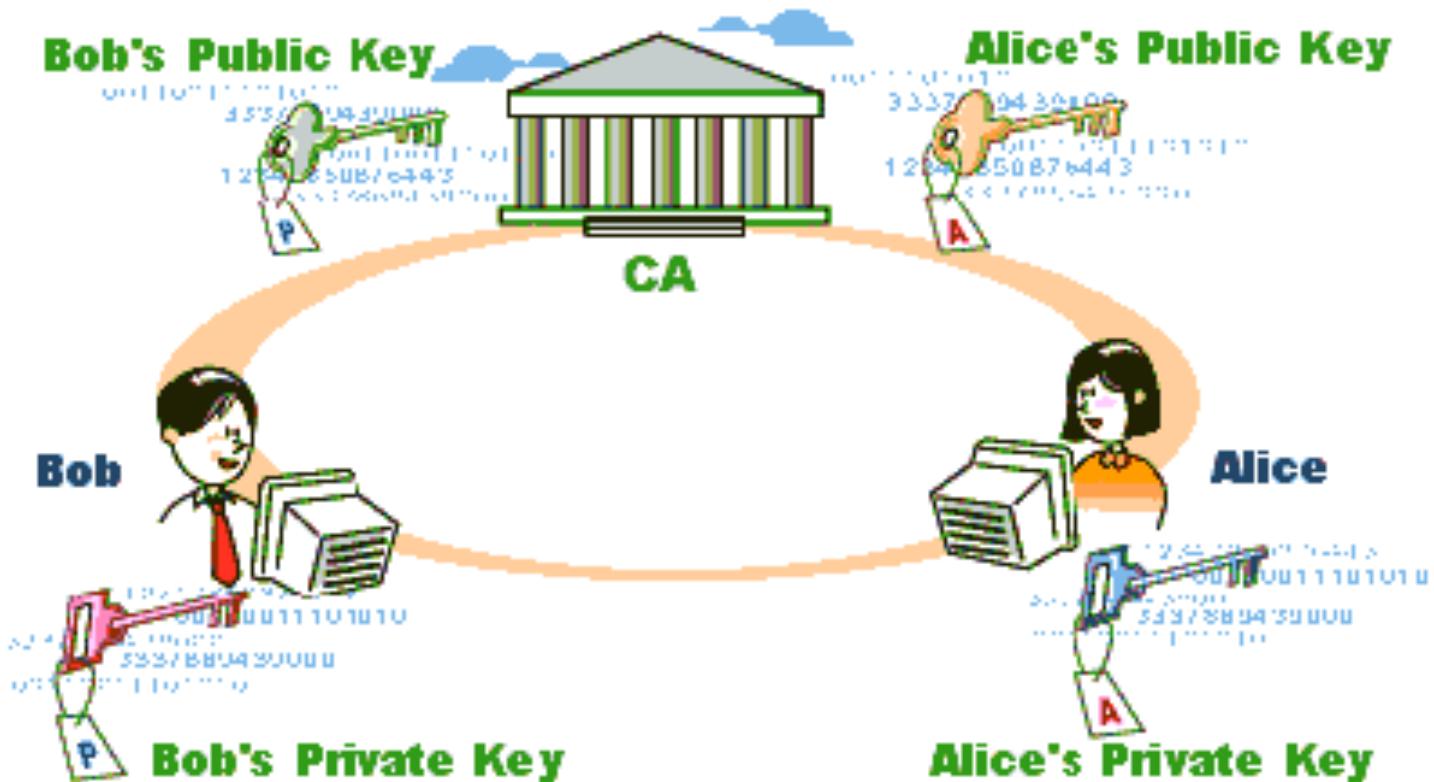
Challenge



"On the Internet, nobody knows you're a dog."

- How to safely collect public keys of Alice, Ted, Mike and so on.
- How to trust { 5, 2407 } is a public key of the target web that never visited before?

Certificate Authority

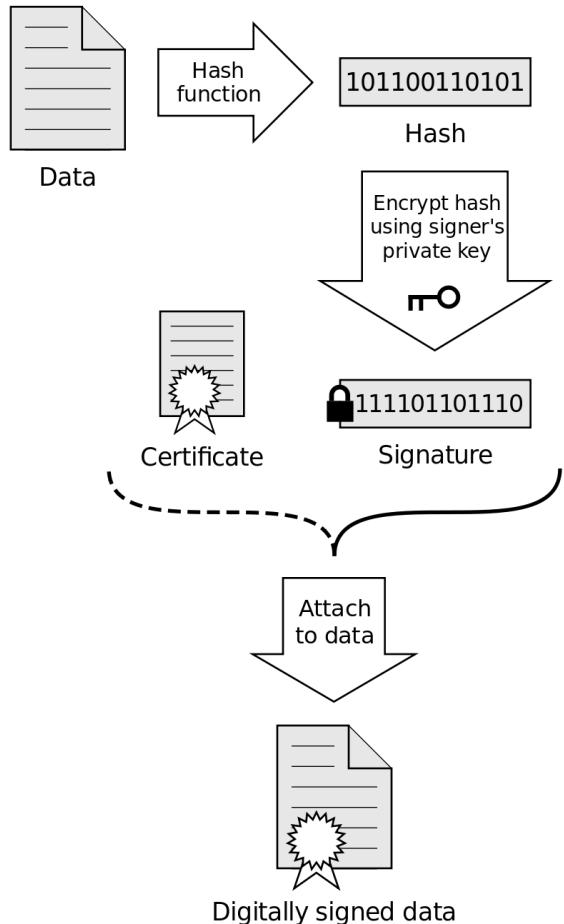


<https://www.comodo.com/resources/small-business/digital-certificates5.php>
<https://www.jspape.com/blog/an-overview-of-how-digital-certificates-work>

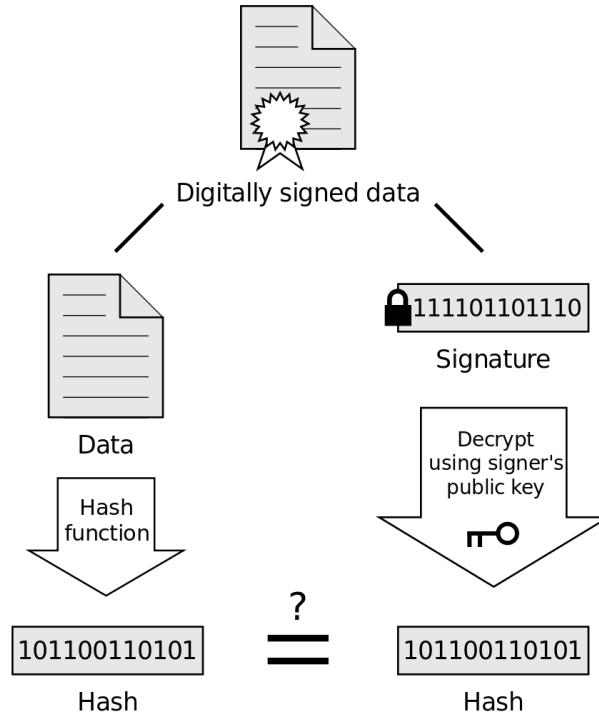
Digital signature



Signing

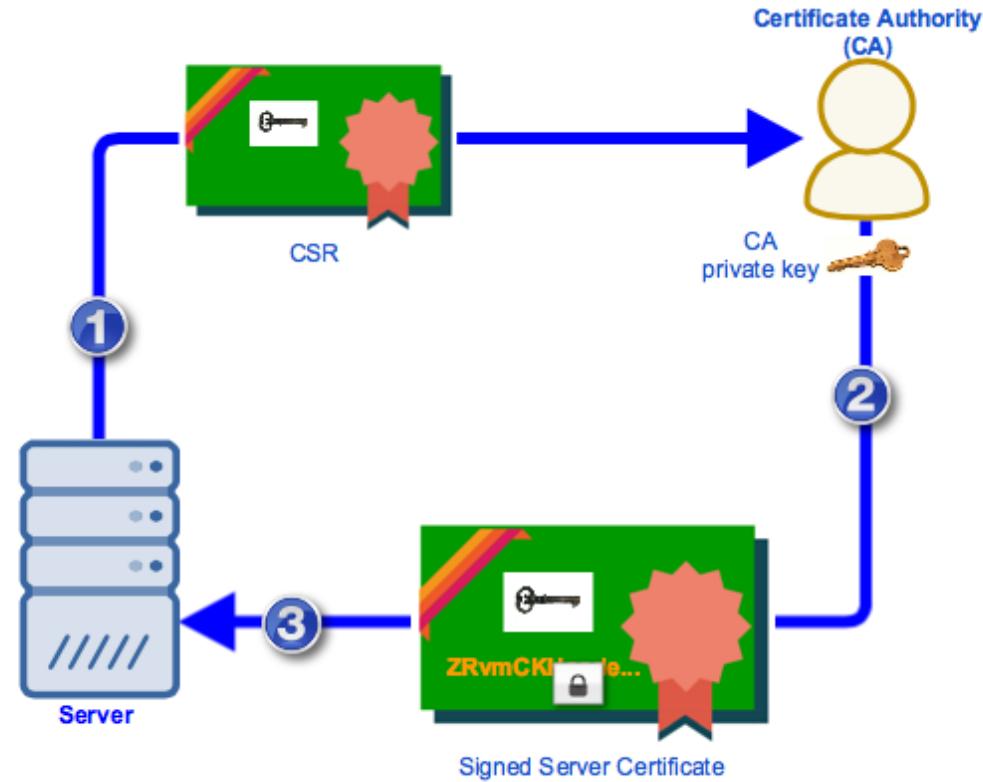
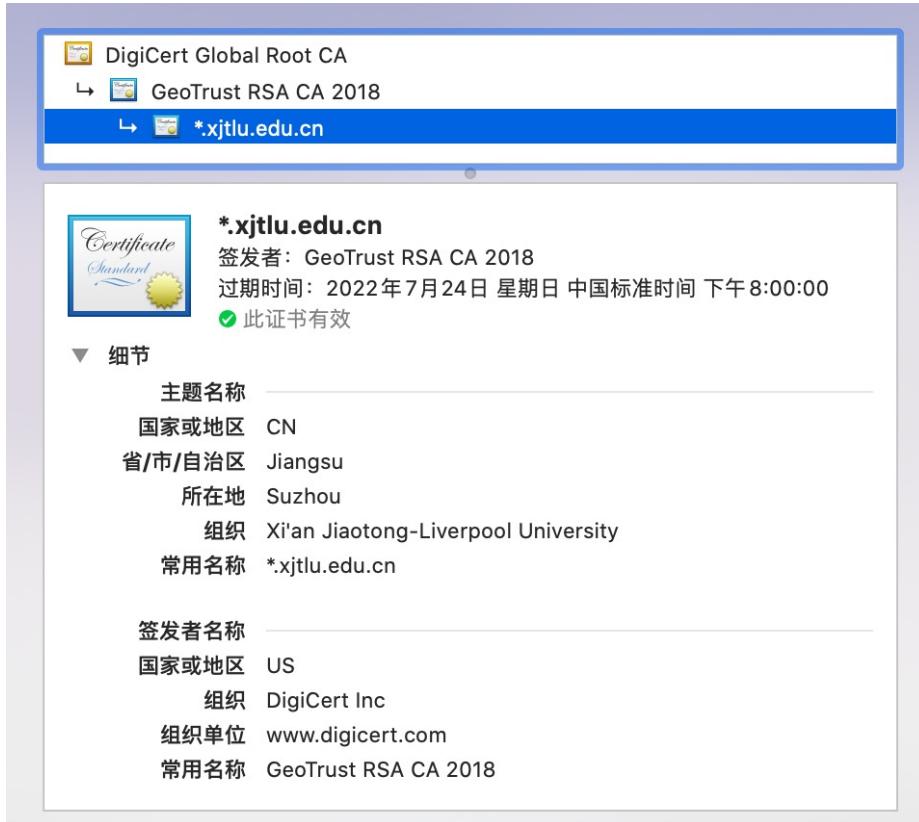


Verification



If the hashes are equal, the signature is valid.

The certificate



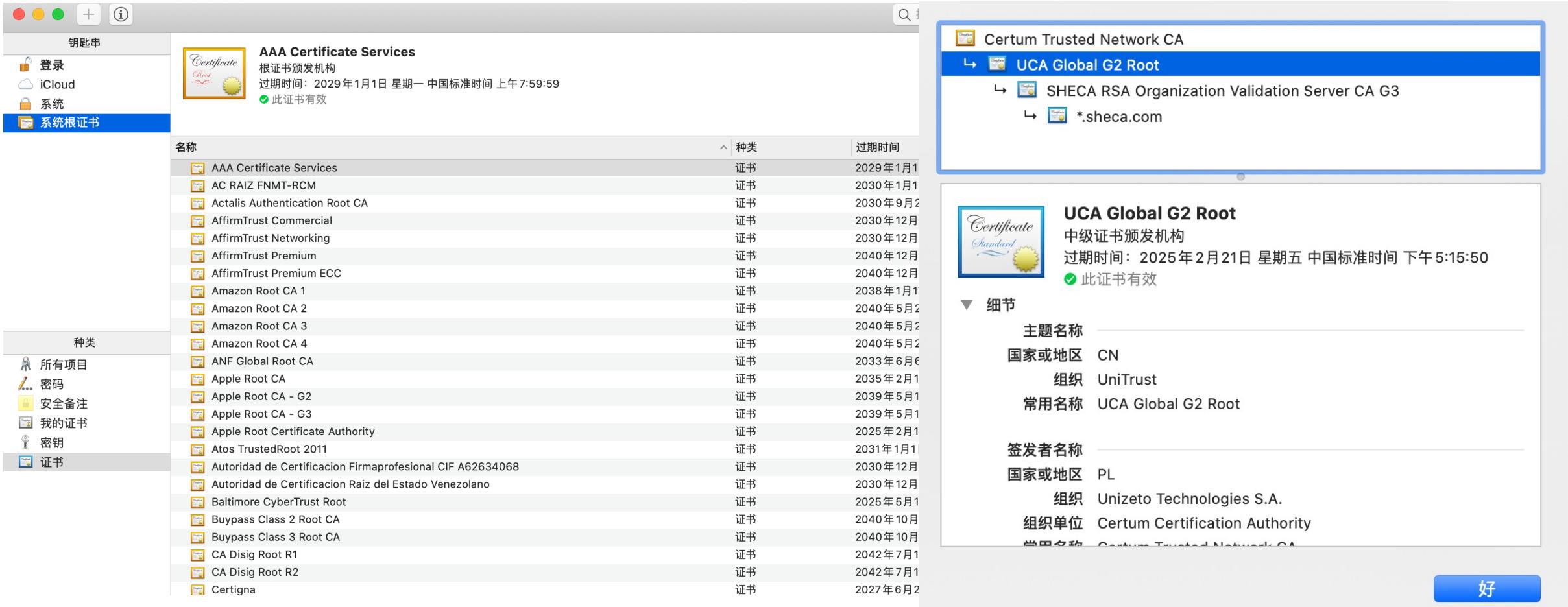
- Webmaster create the key pairs and only send the public key to CA for registration.
- CA need to verify the authority of CRS application.

<https://www.comodo.com/resources/small-business/digital-certificates5.php>

<https://www.jspape.com/blog/an-overview-of-how-digital-certificates-work>

<https://www.myssl.cn/tools/>

Major CA in our browsers



- Dominated by US and European companies.
- 上海CA has been accepted by most browsers.

ITU-T X.509

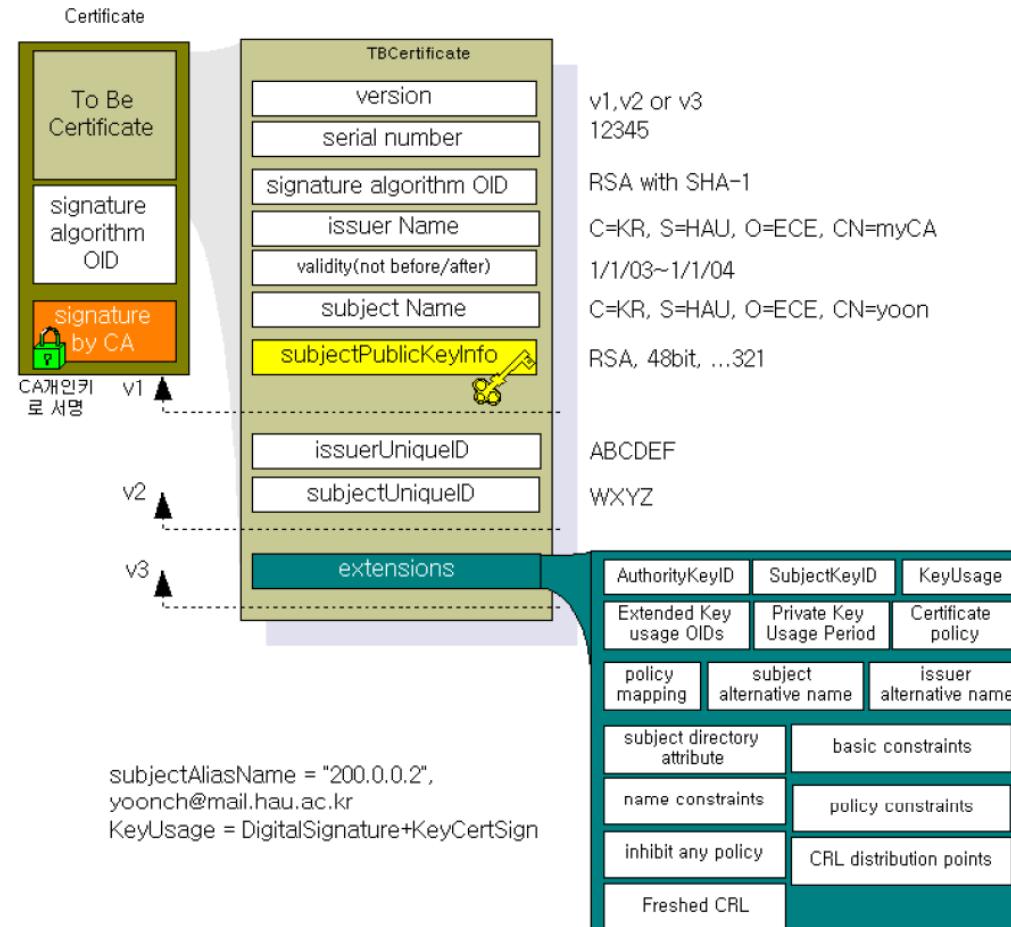
```

SectigoRSADomainValidationSecureServerCA.crt

-----BEGIN CERTIFICATE-----
MIIGEZCCA/ugAwIBAgIQfVtRJr2uhHbdBYLxFMNPzANBgkqhkiG9w0BAQwFADCB
iDELMakGA1UEBhMCVVMxExARBgNVBAgTCk5ldyBKZXJzZXkxFDASBgNVBAcTC0pl
cnNleSBDaXR5MR4wHAYDVQQKEvUaGUgVVNFUlrSVVNUIE5ldHdvcmsxLjAsBgNV
BAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmawNhgdGvbIBBdXRob3JpdHkwHhcNMTgx
MTAyMDAwMDAwWhcNMzAxMjMxMjM1OTU5WjCbjzELMAkGA1UEBhMCR0IxDgAZBgNV
BAgTEkdzyWf0ZXIgTWFuY2hlc3RlcjEQMA4GA1UEBxMHDw0dV0w0aDwvIFJTQSBEb21haW4g
ChMPU2VjdGlnbyBMaw1pdGVkMTcwNQYDVQQDE5TZWNoaDwvIFJTQSBEb21haW4g
VmFsawRhdGvbibTZWN1cmUgU2VydmyvIENBMBIBiJAnBgkqhkiG9w0BAQEFAAOOC
AQ8AMIIIBcgKCAQEA1nMz1tc8INAA0hdFuNY+B6I/x0HuMjDJsGz99J/LEpgPLT+N
TQEMgg8Xf2Iu6bhIefsWg06t1zIlk7cHv7lQP61Mw0Aq6Tn/2YHKHxYyQdqAJrkj
eoCgHuP/IJo8lURvh3UGKEC0pmMWCRAlIzT3YCPb11RFGoKacVPAXJpz90TTG0E
oKMbg6xmrtxZFN3ifmgg0+1YuWQJDgZkW7w33PGfKGioVrCSo1y4u4C8bsk
Haswha6vsC6eep3BwEICc4gLw6uBK0u+QDrTBQBbw4VCsmT3pDCg/r8uoydajotY
uk3DGReEY+1vv2Dy2A0xHs+5p3b4eTlygxFFQIDAQABo4IBbjCCAWowHwYDVR0j
BBgwFoAUU3m/WqoRs9Ug0HYm8Cd8rIDZsswHQYDVR00BBYEFI2MXsRURyRhd+mb
+ZsF4bgBjWHhMA4GA1UdDwEB/wQEAWIBhjASBgNVHRMBAf8ECDAQAH/AgEAMB0G
A1UdJQQWMBQGCCsGAQUFBwMBBggRbgEFBQdcAjAbBgNVHSAEFDASMAYGBFUdIAAw
CAYGZ4EMAQIBMFAGA1UdHwMEcwRaBDoEGGP2h0dHA6Ly9jcmwudXNlcnRydXN0
LnNvbS9VU0VSVHJ1c3RSU0FDZk0aWZpY2F0aW9uQXV0aG9yaXR5LmNyDB2BggR
BgEFBQcBAQRqMggwPwYIKwYBBQUHMAKGM2h0dHA6Ly9jcnQudnRydXN0LnNv
b59VU0VSVHJ1c3RSU0FBZGRUcnVzdENBLmNyDAhBgEFBQcwAYYzaH0cDov
L29j c3AudXNlcnRydXN0LnNvbTANBgkqhkiG9w0BAQwFAAOCAgEAMr9hvQ5Iw0/H
ukDN+jx4GQHcEx2Ab/zDcLSmjEzmldS+zGea6TvVKqjUAxaPgREHzSyRHxVbB
7RM2kYb20VG/Rr8PoLq0935JxCo2F57kaDL6r5R0Vm+yezu/Coa9zcV3HA040LGi
H19+24rcRki2aArPsrw04jTKZ6k4Zgle0rj8nSgf0AnwnJ0Kf0hPHzPE/uLMUx
RP0T7dwBqWlod3zu4f+k+TY4CFM5ooQ0nBnzvg6s1SQ36yOoeNDT5++SR2Ri0Slv
xvcRviKfxmZEJCa0EDKNyJ0uB56DP1/Z+fVGjm0+wea03KbNIaiGCpXZLoUmGv38
sbZXQm2V0TP2RQGgkE49Y9Y3IBbpNV9lXj9p5v//cWoasm56ekBYdbqbe4oyAL
l6LFhd2zi+WJN44pDfwGF/Y4Qa5C5BIG+3vxhFoYt/jmPQT2BVPi7Fp2RBgvG0q
6jG35LWj0h5bJuMLe/0CjraZwtiXWTb2qHSihrZe68Zk6s+go/lunrotEbaGmAhY
LcmsJWTyXnW00MGuf1pGg+pRyrbxmRE1a6Vqe8YAs0f4vmSyrcjC8azjUeqkk+B5
y0GBQMkKw+ESPMFgkU0XwIlCypTPRpgSabuY0MLTDXJLR27lk8qyKG0HQ+SwmJ4K
00u/I5sUKUErmgQfk3xxzLIPK1aEn8=
-----END CERTIFICATE-----

```

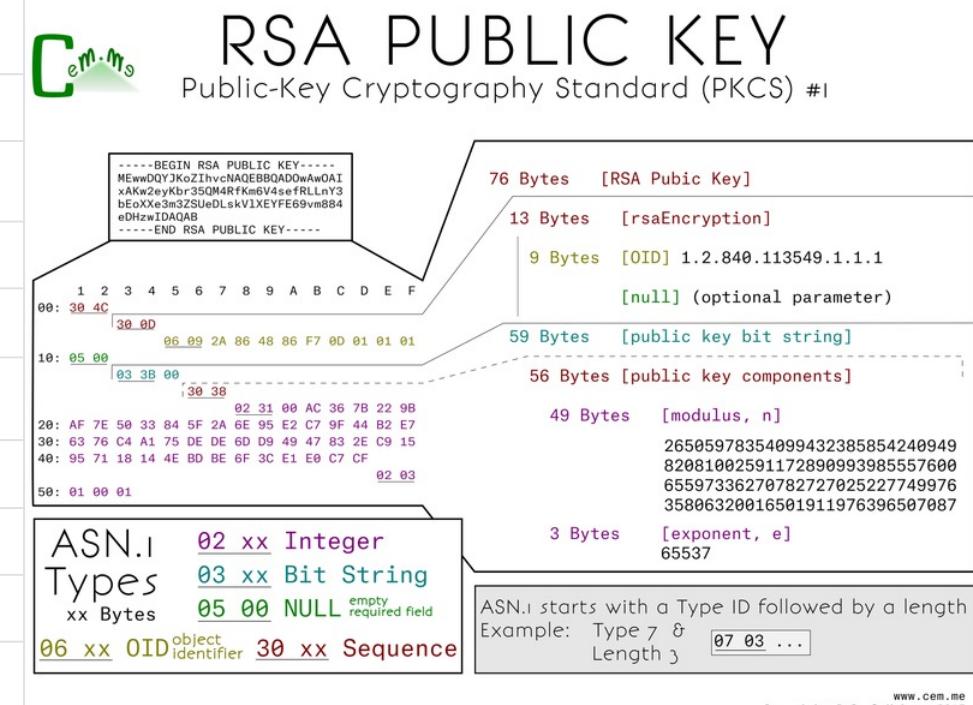
36



<https://www.itu.int/rec/T-REC-X.509/en>

PKCS (Public-Key Cryptography Standards)

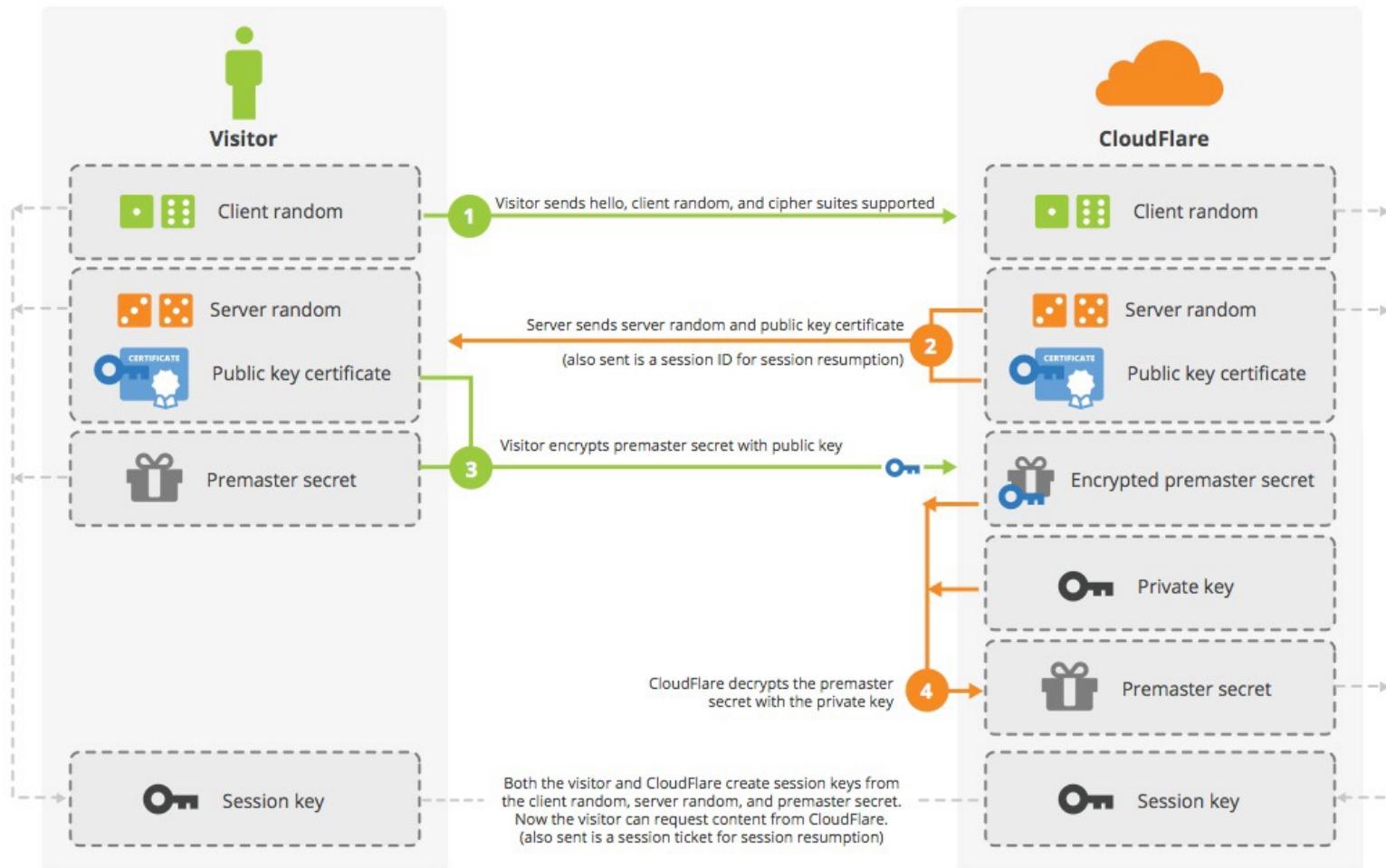
No.	PKCS Title	Comments
1	RSA Cryptography Standard	
2,4		incorporated into PKCS #1
3	Diffie-Hellman Key Agreement Standard	superseded by IEEE 1363a.
5	Password-Based Cryptography Standard	
6	Extended-Certificate Syntax Standard	never adopted
7	Cryptographic Message Syntax Standard	superseded by RFC 3369
8	Private-Key Information Syntax Standard	
9	Selected Object Classes and Attribute Types	
10	Certification Request Syntax Standard	
11	Cryptographic Token Interface Standard	referred to as CRYPTOKI
12	Personal Information Exchange Syntax Standard	
13	(reserved for ECC)	never been published
14	(reserved for pseudo-random number generation)	never been published
15	Cryptographic Token Information Syntax Standard	



<https://www.educba.com/pkcs/>
<https://www.encryptionconsulting.com/public-key-cryptography-standards/>

Actual https

SSL Handshake (RSA)

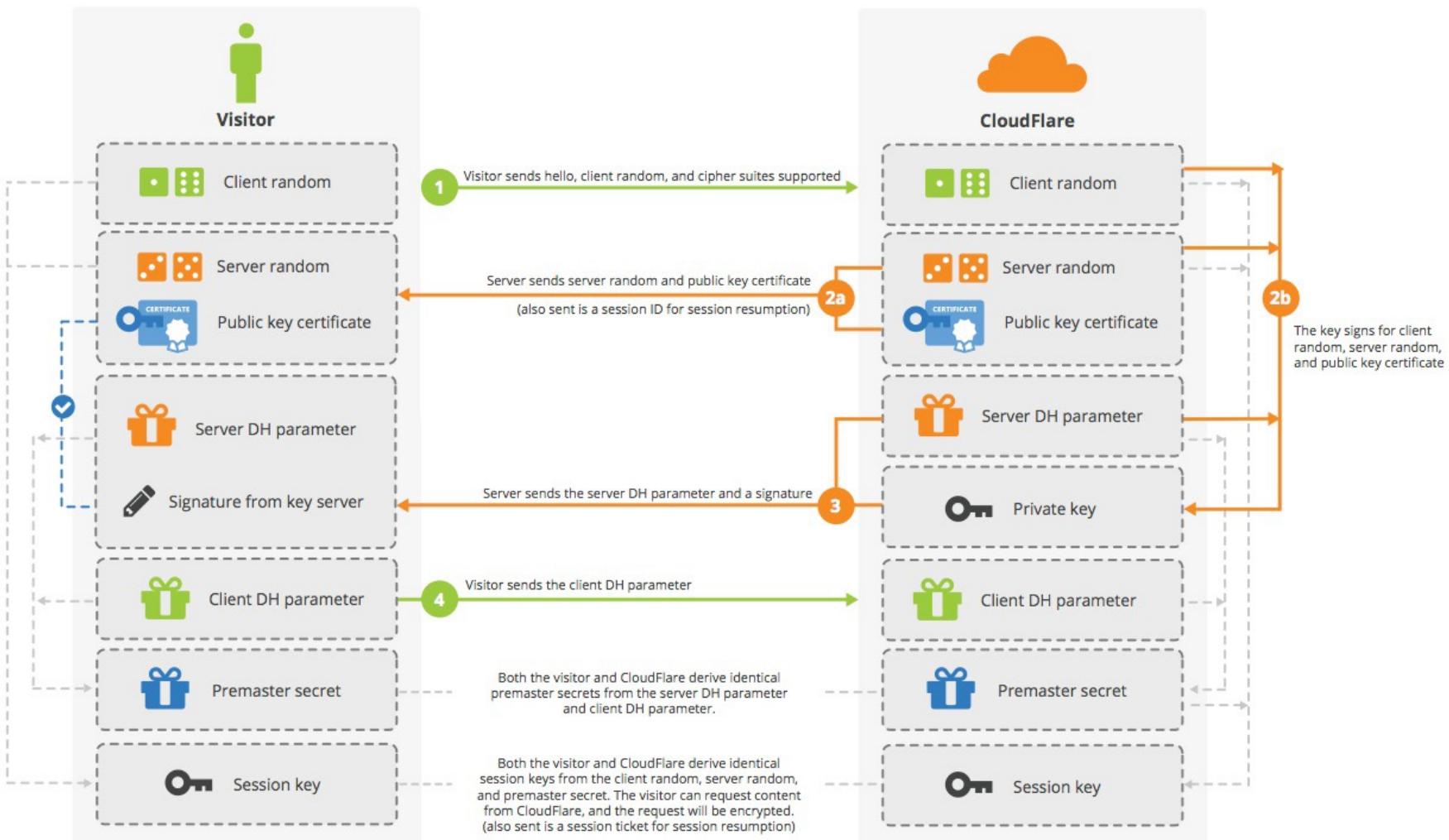


- Session key is generated by server random, client random and pre-master

Actual https

SSL Handshake (Diffie-Hellman)

Handshake



- DH algorithm is used to further enhance the security of pre-master.

Transport Layer Security (TLS) Parameters

↳ Cipher Suites (26 suites)

```
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)
Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)
Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
```



- SSL (Secure Sockets Layer) standard for the "s" in Https.
- SSL has 1.0, 2.0 and 3.0 version.
- A new name TLS (Transport Layer Security) replaced SSL.
- Currently TLS1.3 is the latest version and TLS1.2 is still widely used.
- Cipher suite is an important concept, it contains the method to exchange pre-master, the digital sign algorithm of server, the symmetric encryption algorithm and block cipher modes.
- For example, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 means using DHE to exchange the pre-master, the digital sign is RSA algorithm, AES_256 is the symmetric encryption algorithm and the block cipher mode is GCM.
- ECDH means using EC (math) to do the DH algorithm.
- ECDHE means the session key need to be replaced after certain packages.

<https://www.jianshu.com/p/580e92dc4fdd>

<https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml>

<https://blog.csdn.net/herongoal/article/details/83414888>

MAC - Message Authentication Code

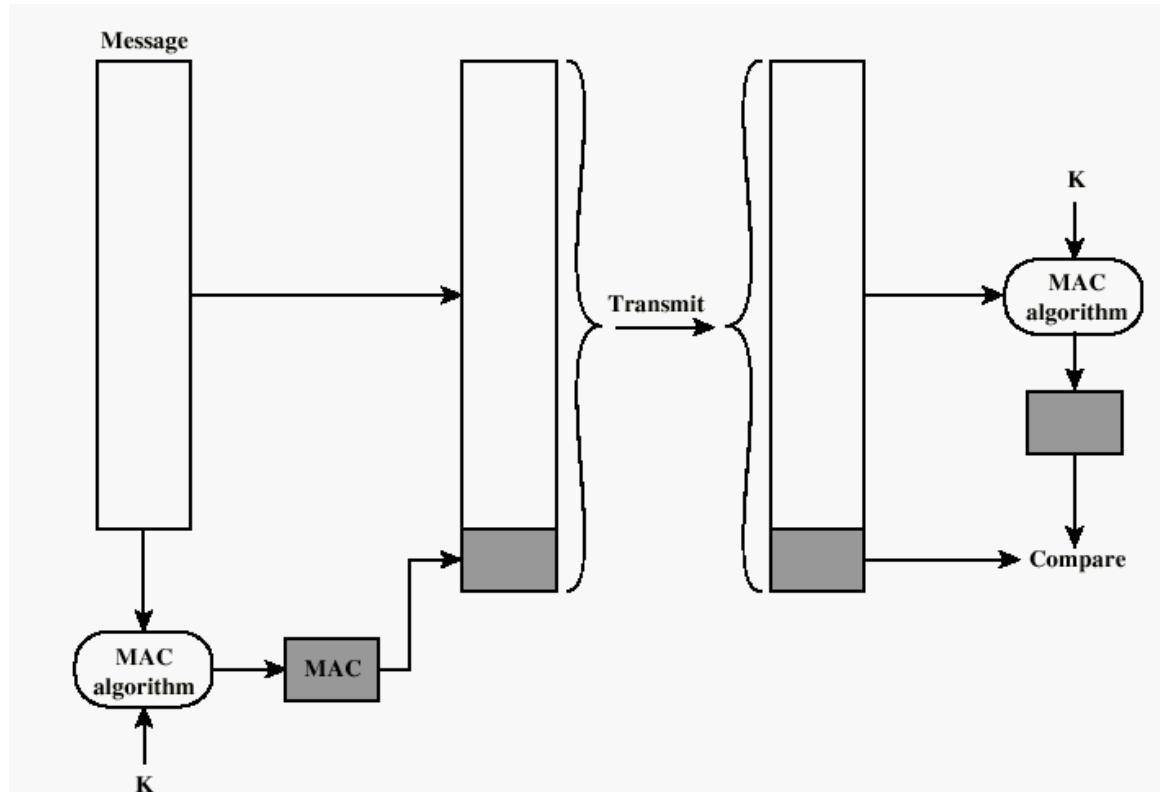
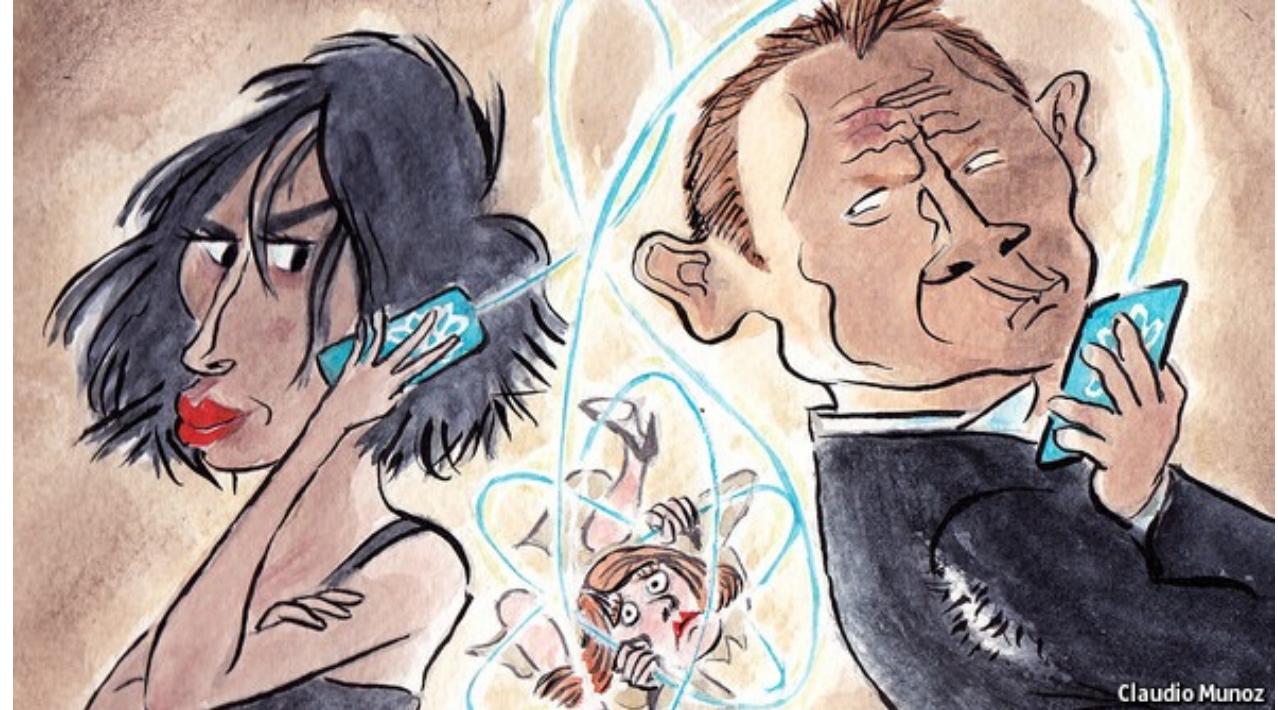
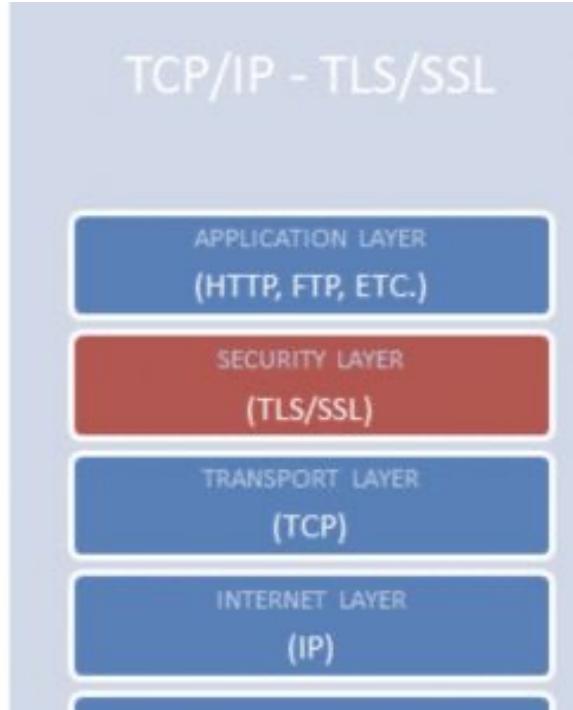
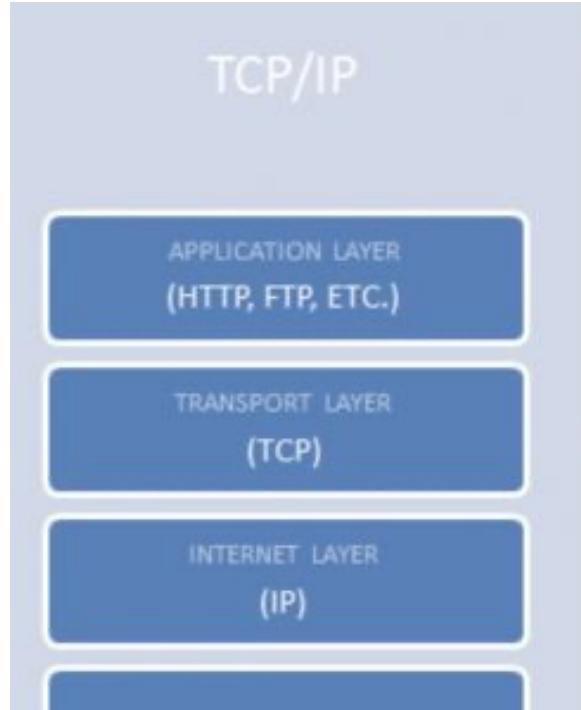


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

- In TLS, MAC algorithm of symmetric encryption is also a part of cipher suite.
- MAC means how to check the integrity of a message, normally a HASH function.

Summary of SSL/TLS

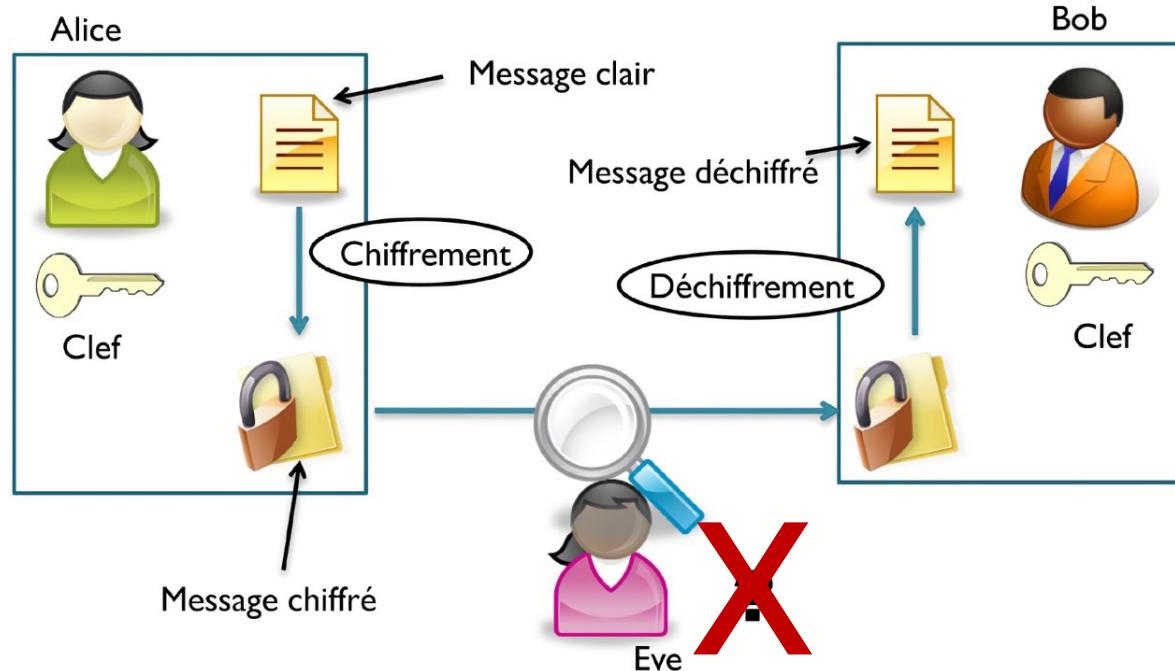
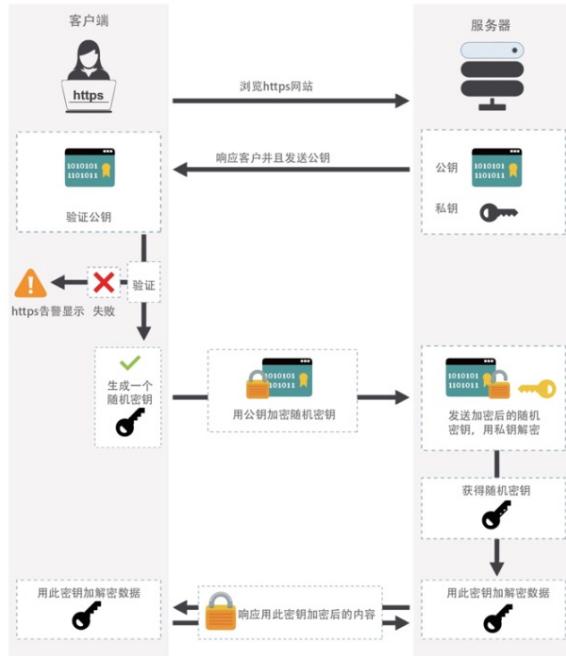


- TLS is not limited to Http.
- TLS can also apply for FTP, SMTP ...
- TLS cannot work if only use symmetric algorithms or otherwise, it combines both.

It seems Eve is out!

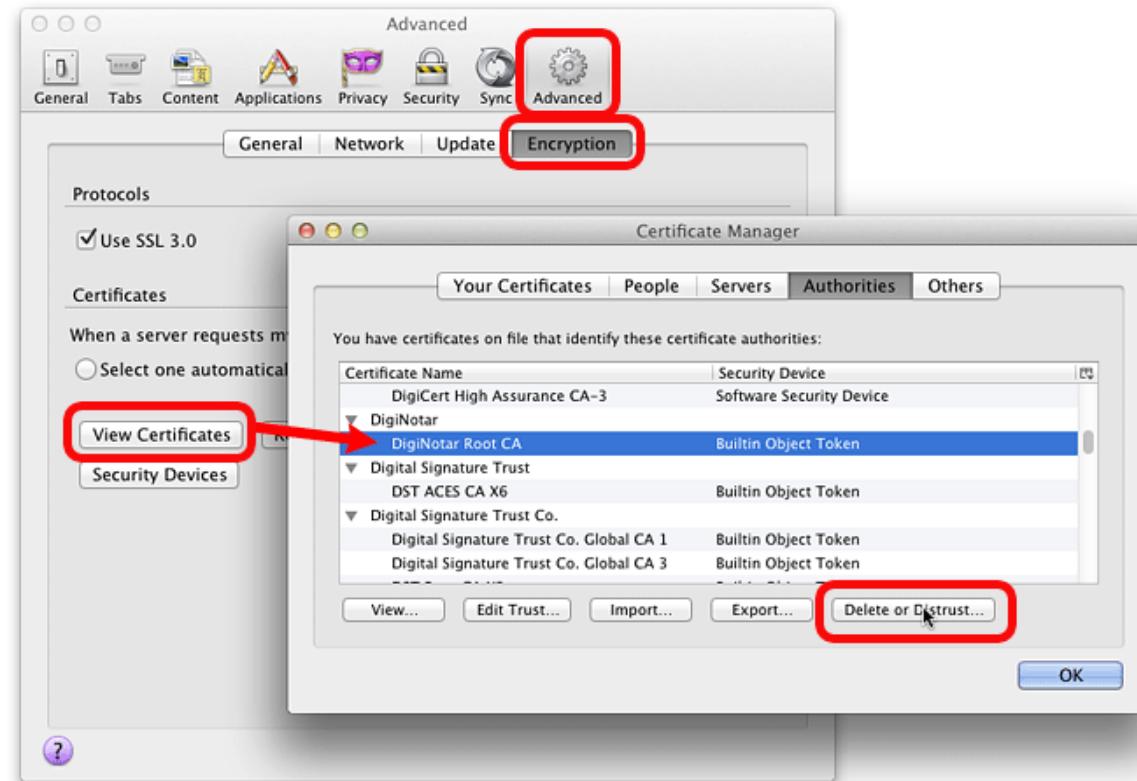


RSA密钥交换



- Remember, the biggest risk is “**We think we are safe!**”

Be attention to this



- CA DigiNotar has been hacked and fake “google” was online in 2011

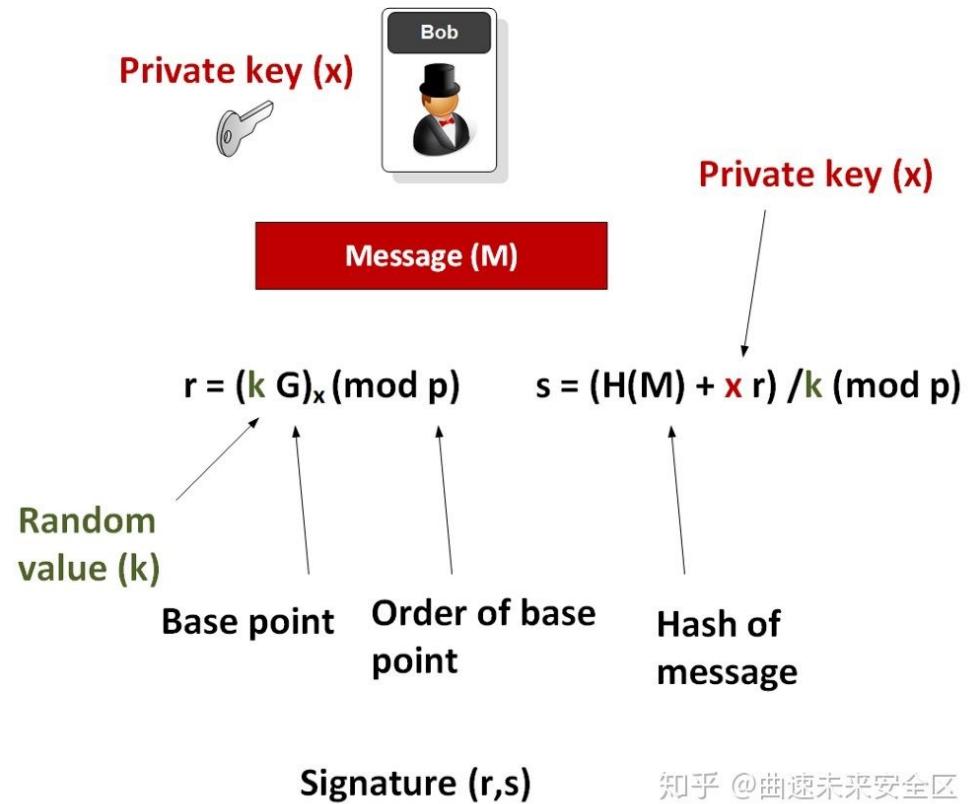
<https://www.zdnet.com/article/diginotar-files-for-bankruptcy-following-hack-attack/>

How about, the private key is **disclosive!**



- It is time to **decrypt** all previous securities!

Tools cannot guarantee safe, but with people



- **Again**, But more important thing is about people and related regulations.
- Sony PS3 use a fixed “random” number, the door opens for everyone.

<https://zhuanlan.zhihu.com/p/49568984>



Password or account credential

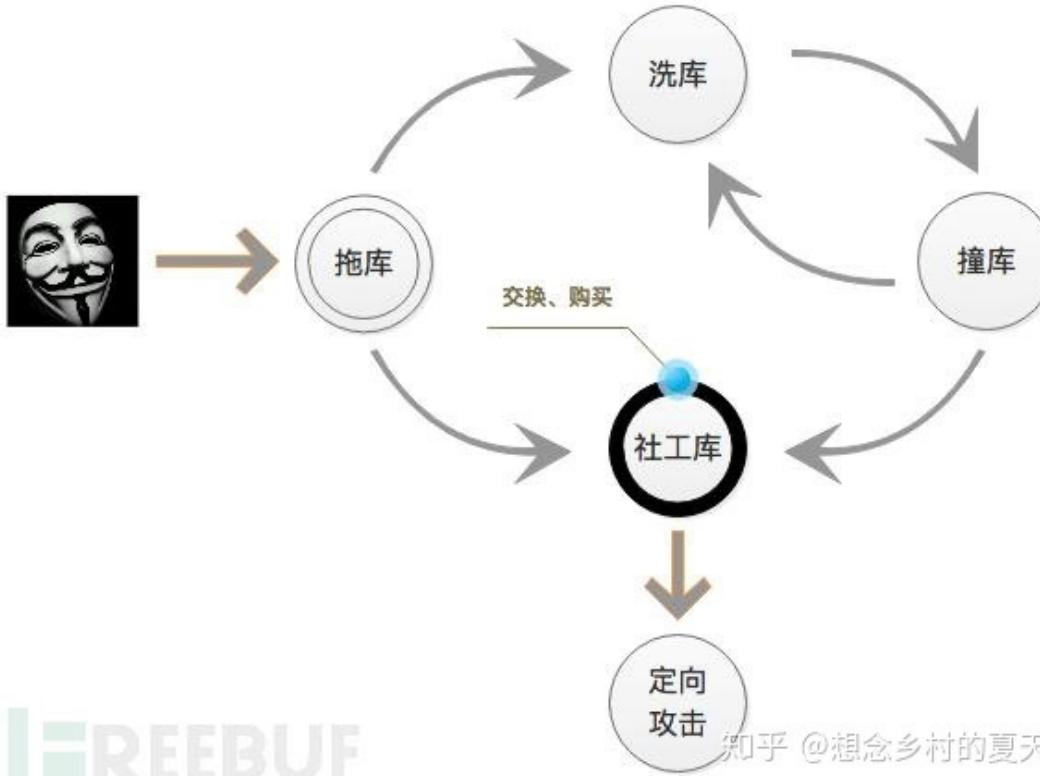
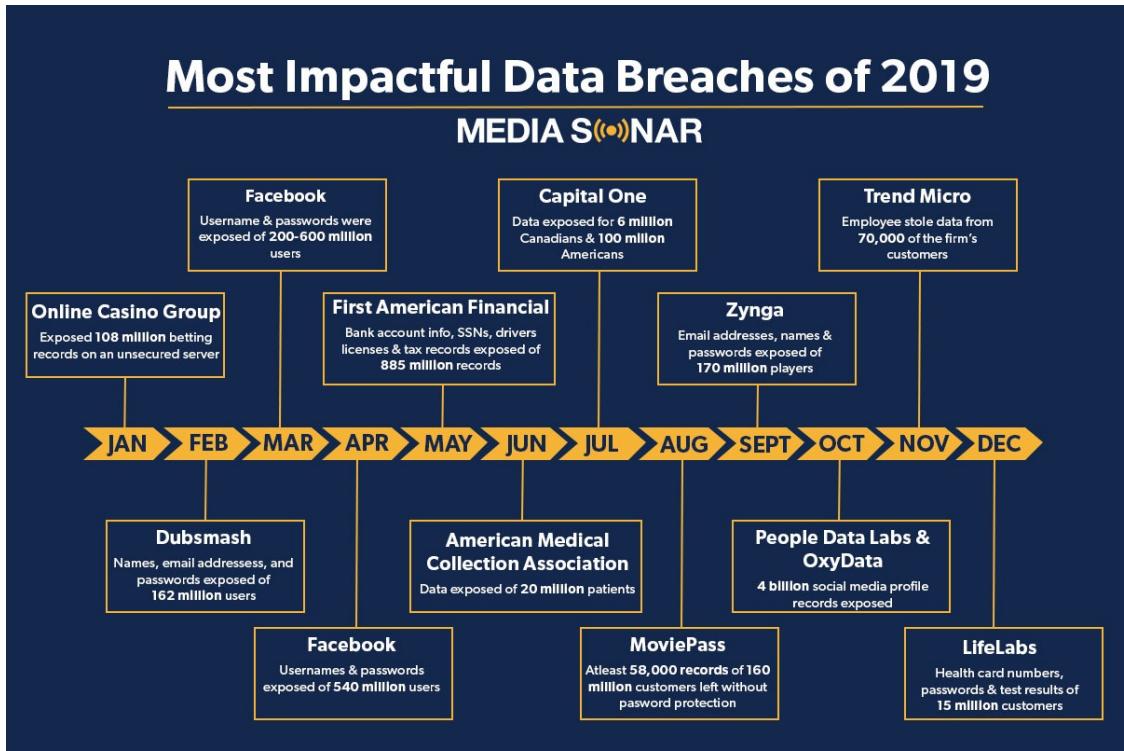


- **Password:** something that enables one to pass or gain admission
- **Credential:** testimonials or certified documents showing that a person is entitled to credit or has a right to exercise official power

Username + password is the most widely used authority credential on internet

<https://www.merriam-webster.com/dictionary/password>

Attacks never sleep



FREEBUF

知乎 @想念乡村的夏天

- Harvard Business Review: "*You Can't Secure 100% of Your Data 100% of the Time*"
- But we need to do something to make it hard or worthless.

<https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time>

Never store passwords in plain text



ID	LoginName	LoginPwd	Status	IsDel	UpdateTime	EName
44	1810	1563	2E 53	3	False	NULL
45	hellc	5	12 56	3	False	NULL
46	137	1491	pr se	2	False	NULL
49	130	202	12 567	3	False	NULL
51	186	1338	01 121	3	False	NULL
52	137	1417	11 072	3	False	NULL
53	158	605	06 dV	3	False	NULL
54	151	4073	12 56	3	False	NULL
55	151	4072	12 56	3	False	NULL
56	adm	pr seit	131	False	NULL	NULL
58	130	738	12 56	3	False	2014-7-15 11:1...
59	135	1117	12 56	2	False	NULL
61	1570	1567	12 56	3	False	2014-7-25 11:3...
62	wft	wf 318382	1	False	NULL	NULL
64	w18	35709	12 56	2	True	NULL
65	186	709	12 56	3	True	NULL
66	180	1566	ss 7198	3	False	NULL
67	189	1919	ty 2013	3	False	NULL
69	158	1858	65 21	2	True	NULL
70	158	1859	65 21	2	True	NULL
71	138	1351	65 21	2	False	NULL
72	1850	1213	00 33	2	False	NULL
73	138	817	65 21	2	True	NULL
74	133	817	65 21	2	True	NULL
75	185	228	12 56	3	False	NULL
76	1850	517	12 56	3	False	NULL
77	1870	1599	68 0810	3	False	NULL
78	188	132	00 34	3	False	NULL
79	186	971	40 10	3	False	NULL
80	186	1891	76 30	3	False	NULL
81	132	868	wf 3752256	3	False	NULL
82	188	946	52 23xiyu	3	False	NULL
83	189	888	65 21	2	False	NULL

- **Password** is only for comparison.
- On design, even the Admin should **NOT** have any chance to access customers' passwords in plain text.
- **HASH** is a good choice while it is **NOT** an encryption algorithm.
- For example, you can read 123456 very easily. But you may not know what does "8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92" means.
- It is SHA256("123456")

http://wy.zone.ci/bug_detail.php?wybug_id=wooyun-2015-095231

Hash collision attack

These following two different 128 byte sequences hash to the same:

55 MD5 Hash: 79054025255fb1a26e4bc422aef54eb4

The differences below are highlighted (bold). Sorry it's kind of hard to see.

 d131dd02c5e6eec4693d9a0698aff95c 2fcab**58**712467eab4004583eb8fb7f89
 55ad340609f4b30283e4888325**f**1415a 085125e8f7cdc99fd91dbdf280373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e2**b**487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080**a**80d1e c69821bcb6a8839396f9652b6ff72a70

and

d131dd02c5e6eec4693d9a0698aff95c 2fcab**50**712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325**f**1415a 085125e8f7cdc99fd91dbd**7**280373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e2**34**87da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1e c69821bcb6a8839396f965**ab**6ff72a70



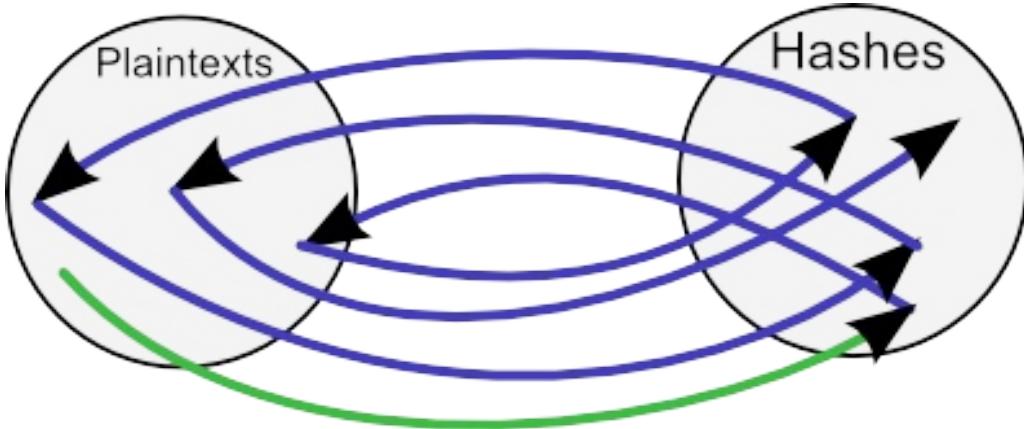
- Dr. 王小云 proved collisions can be found in MD5, SHA-1 algorithms
- She lead the design of SM-3

<https://baike.baidu.com/item/%E7%8E%8B%E5%B0%8F%E4%BA%91/29050>
<https://zhuanlan.zhihu.com/p/377468857>

Hash only is NOT safe



Software: RainbowCrack 1.8
 GPU: AMD Radeon RX 5700 XT
 Memory: 16 GB DDR4
 Disk: SSD with Sequential File Read Performance 1600 MB/s



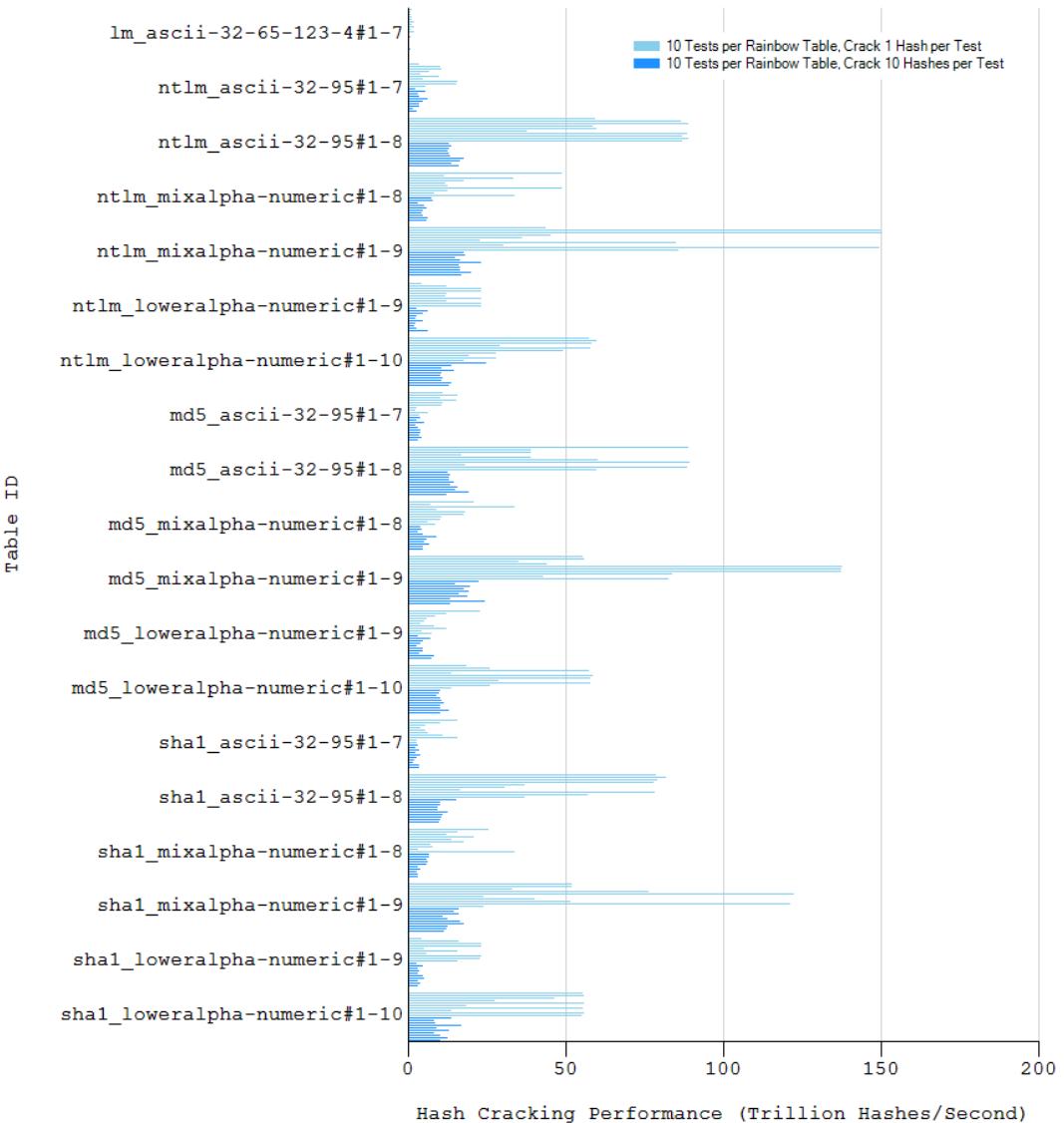
- Rainbow table help to speed up the hash finding.
- Add “**salt**” can improve the difficulty.

<https://kestas.kuliukas.com/RainbowTables/>

<https://www.ionos.com/digitalguide/server/security/rainbow-tables/>

<https://www.jianshu.com/p/732d9d960411>

<http://project-rainbowcrack.com/table.htm>



Salt can NOT against database searching

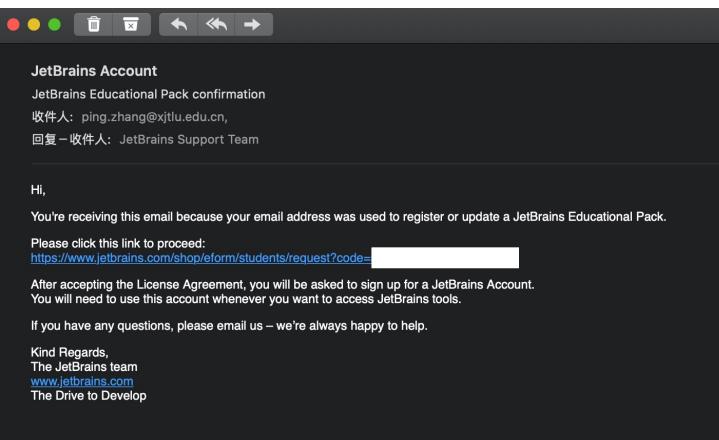
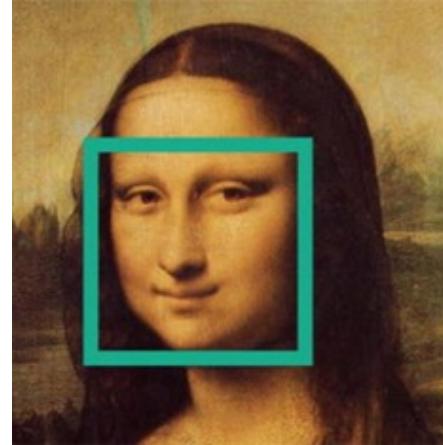
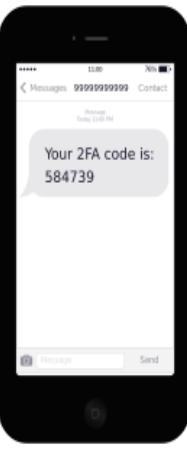
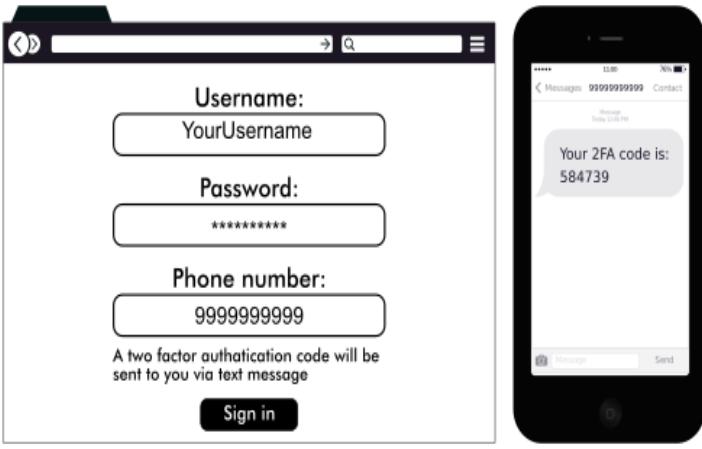


2017-08-09: ab11e98ec937160da094cfb5211dad4b75a73727f0faad29410462fa42441c . /inputbreach/500k+ComboList[Netflix,Paypal-Origin,Amazon].txt 3.1N
2017-08-09: 74be21c25cf46e6ba82c5cd04dc64b03937deb554c61843dbbd80d92d3186f . /inputbreach/accounts.txt 9.9M
2017-08-09: 52548df0f7cc735bf1bad8b3448cce864b60e384e63eaa59c4d7f8a30d71a43 . /inputbreach/FRESHOVER1,2+M.txt 40M
2017-08-09: f7c1579e5fe77df4c92246727f99e69a69e15d1793c6ed0e6d17a8ccb15d . /inputbreach/500k+ComboList[Netflix,Paypal-Origin,Amazon].txt 3.1N
2017-10-02: 52f640e95015b6b060eb075fe2a8776395e2e38cd13972ad251d3b1ae89298 . /inputbreach/000webhost_13ml_plain_Oct_2015_filtered.txt 4849
2017-10-02: 2852052b0636cb590eb00b6d6808e0c1a4660b9473931e59692b212d2a825d0e . /inputbreach/surgery.com-641009_surgery.com-users_30.10.2016.txt 36K
2017-11-08: ea499b03d11cb00097cc6d19c55c48e0dd5ed56e591a12fc80d2c4239cb950 . /inputbreach/10workingminecraftaccounts.txt 4.0K
2017-11-08: 27426d4e35547a54514a404a5c18bf8e05e44d42bb7c5fe8767d4f41ee517a . /inputbreach/1394store.com_LEAKED_DATABASE_filtered.txt 612P
2017-11-08: d4014c9281d742b63853f2398e8fb6fcd47919da3d44e1287a20e5e1415 . /inputbreach/36kmember_filtered 1.1M
2017-11-08: 5a3f58c957935642422255ab9d9e265318f921147b04093d2ea8f5f7f44c8ae22 . /inputbreach/77K201M
2017-11-08: 56e2fa4a0708b3b3cb9506e31ea698e3ad1f37065a346617b819d1617e087 . /inputbreach/99farme.com_filtered.txt 36K
2017-11-08: 718e7b552c9c14f80b6c74087a9adc5faa144288be0889d2d82b98e201ad6 . /inputbreach/Alancristea.txt 8.0K
2017-11-08: 5fb01355d6a98a54c61fa08341960bcb943601a3c9b0f03721b55b7b632a . /inputbreach/Balancek.txt 168K
2017-11-08: bdc490aab2dc010ea1716b7b4a4b9038723ebd89ee5c3ac2348bc21b2b0c48 . /inputbreach/Barbellith_Users_credentials_filtered 208K
2017-11-08: cf492442dc17b2587436383b1fb8bcb780311206958979995735d65b7b . /inputbreach/BitcoinLxter_filtered.txt 92K
2017-11-08: 4f650ace9bfa563f50b2c14e7996e6cb1ca0ab46z2c29e093657a2fafaf27228 . /inputbreach/CSGameSers.Com.txt 504K
2017-11-08: 4494d26841coeb60e0e03d4865b5b6e6079fc4d18a3899416629d72367cc53 . /inputbreach/DBDBDBB_filtered 760K
2017-11-08: 152e7922a171f26bd6176748c3f6bd9f71a0ee5c5a587915d92bd72fd . /inputbreach/Delicious_Takoyaki_filtered.txt 2.8M
2017-11-08: 833b2b89425399187a064a4d3d439c57c02a5c2fba057d8faee56943bc916 . /inputbreach/Fling_filtered 1.3G
2017-11-08: f149eb28038acc1e892d45fa5180613e18143c694648a9d65a66961b52c4 . /inputbreach/LuzSecDelivers_filtered.txt 760K
2017-11-08: e2811cf0657b29476a54757c8a45fe324d078830cc0d2b6eae8b7bcc998 . /inputbreach/RuneScape2k15_filtered 2.8M
2017-11-08: c8f3b090996e57fcdb1861b12f88dcbbcda7a729885beba561e976808a4f60 . /inputbreach/WEBS_filtered 328K
2017-11-08: b75a42d0dc01c1a9a839a179b8d05867f0624195b69dd58480bfad1e592e581 . /inputbreach/myspace.sorted1 1.1G
2017-11-08: 495d7bc8ab649cb298cd031cbc9fe82d959f5e3503a781371b91683434349 . /inputbreach/myspace.sorted10 1.1G
2017-11-08: b5536c830b3171e7c7e1041eba4a4064e09a4fc6da3d998276114ad1753224 . /inputbreach/myspace.sorted2 1.1G
2017-11-08: eb86c21b2dc1657f205b11675de9d6191320c786e1059eae2607d5f59361a . /inputbreach/myspace.sorted3 1.1G
2017-11-08: ef67ccc976b428c2a694757c8a45fe324d078830cc0d2b6eae8b7bcc998 . /inputbreach/myspace.sorted4 1.1G
2017-11-08: f5e59f766c61a458346771871fa7c2c09a571b64ca4fc8910285522a4e4a . /inputbreach/myspace.sorted5 1.1G
2017-11-08: bdbbbfc6258608529da0c06667c3391414aa0475aa03079b05c5bcb0e261 . /inputbreach/myspace.sorted6 1.1G
2017-11-08: dc238d7a170b7352d15518d668c09527d4c524fa36a3031155d5eed11de8a . /inputbreach/myspace.sorted7 1.1G
2017-11-08: b8c9de47be886e584e74b0d9c1dd00a8ca59e423fafe02c16ea8012ab0c2 . /inputbreach/myspace.sorted8 1.1G
2017-11-08: a57b01a4e58a83866c29545d2c1d0e8cd16e98fbbe49d535ce9a121850984710 . /inputbreach/myspace.sorted9 1.1G
2017-11-08: 03998b6ace44f1608c8499790c8a01fd43260f1b2801cf80cbd3b32f0283 . /inputbreach/plaintxt_yahoo_voices_filtered.txt 14M
2017-11-08: 8215639b59b9ca21554ad89c3b046b27464ca80f6931e30c7d5b8d47e8d2a . /inputbreach/redbox_filtered.txt 7.4M
2017-11-08: e738e61b66731c98c5b982930f5b5c94139396e0b7 . /inputbreach/twitter_filtered 1.1G
2017-11-08: 8440cf3377753c9a7aa1b9503e10596d6ded8263801929e693aa823197a85 . /inputbreach/yuporn_filtered 45M
2017-11-09: 0c0dfa65728a366012f00fe06da37e693d11hd932540e9944d3fc9cf0b3402 . /inputbreach/badoo.sorted1 896M
2017-11-09: 8f77ce22d9d9e1209329d7b5f763a95b622727f7a07981b8491843c7078 . /inputbreach/badoo.sorted2 896M
2017-11-09: f1cece7b51a01e717fd4d4a8d803978882d3b2e0e7fa07981b8491843c7078 . /inputbreach/badoo.sorted3 896M
2017-11-09: 8d35ade995ca47f15a2110fb270a7545e50f0a61d7233dec791a9eb4129 . /inputbreach/badoo.sorted4 896M
2017-11-18: c30f1caa24430484eda17b2771cb38f5ad4cdd6415744426cb9e230ded2ed3 . /inputbreach/linkedin110M_1 865M
2017-11-18: 6925d41d3d5bcb96687a3f7a69681372ce88d4f7bd955c07942637e . /inputbreach/linkedin110M_2 865M
2017-11-18: ca973734654654999d7315ad52c69691372ce88d4f7bd955c07942637e . /inputbreach/linkedin110M_3 865M
2017-11-18: 577163674fb8e192329dbe3ac2fcf342a72b6e17a5c684824687615caco . /inputbreach/linkedin110M_4 865M
2017-11-19: 484ab669622447b5780e107d8726203c565d1b241ca6a5940277cb9e6b920 . /inputbreach/tobao 409M
2017-11-19: 14423b8b3e8b99b59756eet156ee58497d3b3d805a386c08d2ae8f3a5213 . /inputbreach/splitl_sorted 91M
2017-11-19: f409e63a064e0d241a9e80d228f1538b3cc4430f2aeb1e20f2d1f437d6ba . /inputbreach/zooksl_sorted 811M
2017-11-19: 25767c72a599cc35596788a1846e1dd586f6d6b6b56a3caf097d1f520ce0 . /inputbreach/zooksl_sorted2 811M
2017-11-28: 5ef0fb35e20685527139e5a0d7971e4497dfdea091a4e69b5f5bda527223 . /inputbreach/17media_sorted 87M
2017-11-28: e74c9c7d93671fd5e382b50bc090913d65c7648480cc096d9458044d8f89d . /inputbreach/2.6MNulledIoEmailPassCombo 74M
2017-11-28: ad139905a2f483803f32a2abc0acd7642f892d3a3387393bce317bcf81a9 . /inputbreach/700KEMailPassForPaypal 20M
2017-11-28: 2814f663d5427090f88a04f620165c5e6a5363d687 . /inputbreach/Neopets 1.1G
2017-11-28: dd0f9ef53085f6d4e79f4cc17c6c8a5b579a2cc05e4541coed269t3f6680 . /inputbreach/bleachforforumdecryptedemailpass 2.6M
2017-11-29: 916823bbcc33dd795b361ce2328661d1a384df2f698356e3dab0d8e3890732 . /inputbreach/lastfm_sorted 1.2G
2017-11-29: 04bc70c03d02e1c3bbcc10ab56567167d10baee55aa1526759f41b9cbacf7 . /inputbreach/tianya 779M

https://www.sohu.com/a/210357960_804262

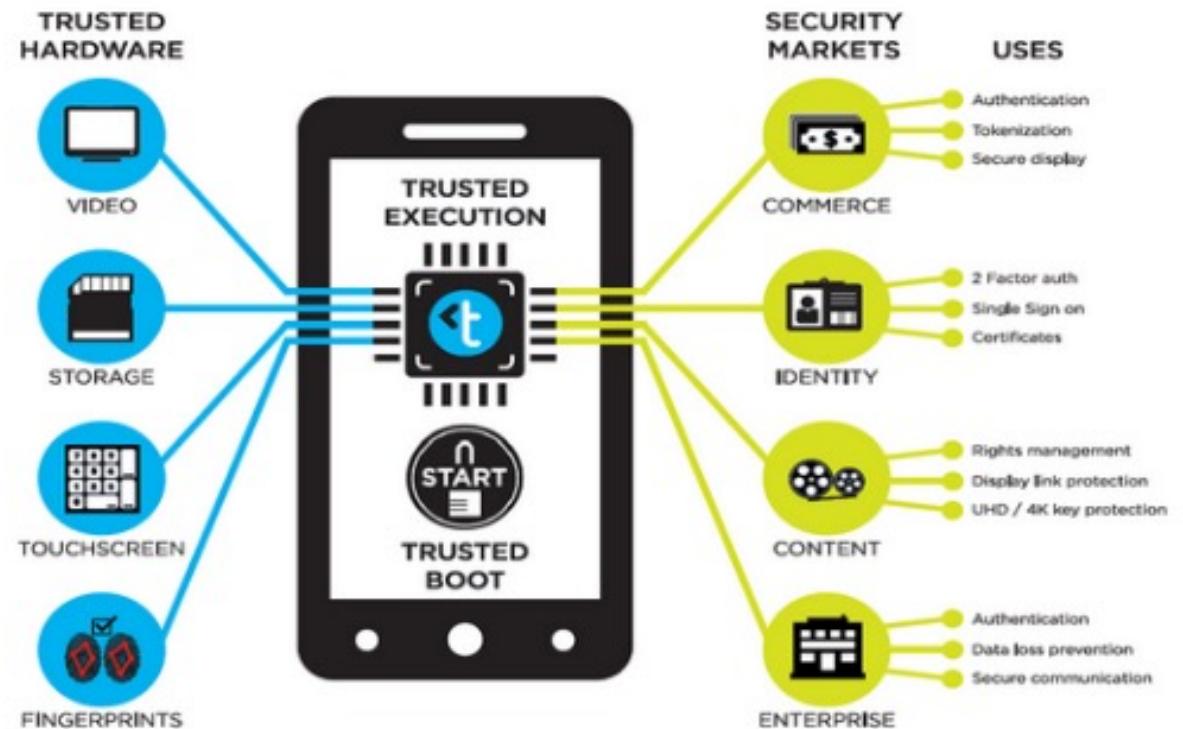
- According to public report, over 1.4 B passwords breach.
- Let customers check if they are in the list.

MFA: Multi-Factor Authentication



MFA is a security system that requires more than one method of authentication to verify user's identity for a login or other transaction.
Normally, 2 factors are used. **2FA** (Two-factor authentication) is a subset of MFA.

And these



- Public Key Infrastructure (PKI) can also be used at client side.
- Normally the private keys are protected by chips.
- CA play an important role in USB stick for PC application

Tencent 'soter'

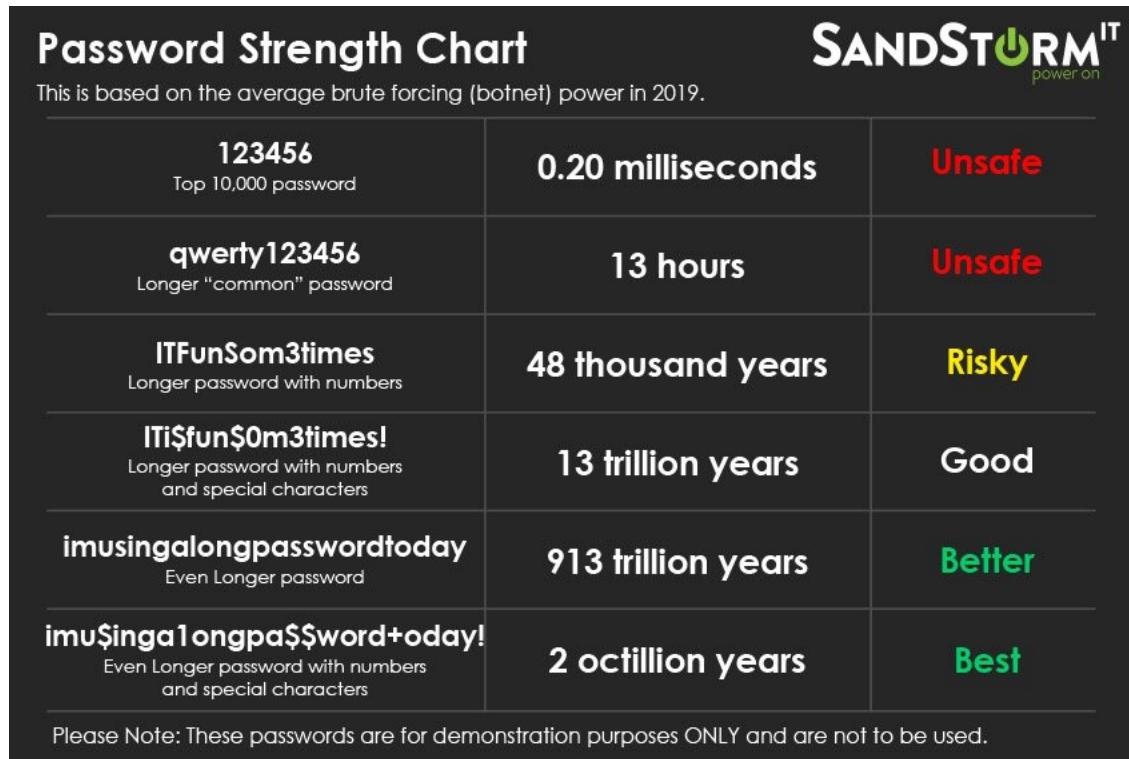


密钥名称	唯一性	作用描述	生成算法	公钥位置	私钥位置
ATTK	设备唯一	验证设备合法性	RSA-2048	TAM Server	RPMB
ASK	应用唯一	验证应用合法性	RSA-2048	第三方应用程序 Server	File system as other keys (加密存储、权限控制)
Auth Key	不限数量, 根据业务需要生成	验证业务逻辑唯一性	RSA-2048	第三方应用程序 Server	File system as other keys (加密存储、权限控制) WeMobileDev

- It is a correct BUT difficult way to go.
- get all mobile vendors' support to send root certificate to Tencent.
- Tencent TAM server play like the root CA server.

<https://github.com/Tencent/soter/wiki>

Some suggestions on Password/Credential



- Weak password is the NO.1 factor.
- Do not install “dangers” APP/software, like 180 * 2.
- If you have to, use the “dangers” software in VM.
- Do not use the same password for different website/APPs, at least add some “salt”.
- Do not register account in “unsafe” websites, for example, those do not use 2FA.
- Do not share password.