



CYBER SECURITY: ESSENTIALS

Daniel Medina — medina@nyu.edu

ADMINISTRATION

Notes: <https://medina.github.io>

Anyone new join?

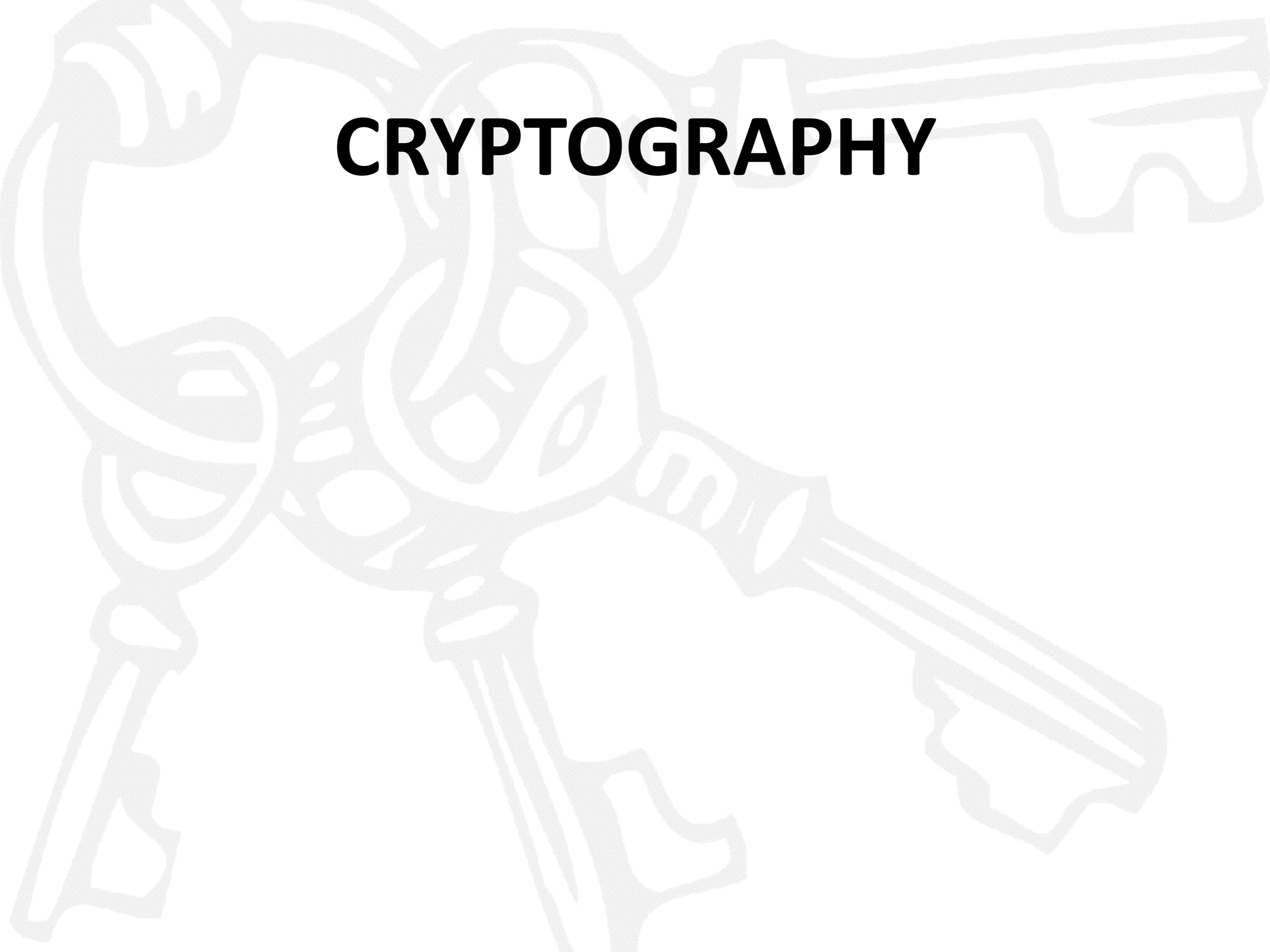


NEWS



RECAP

CRYPTOGRAPHY

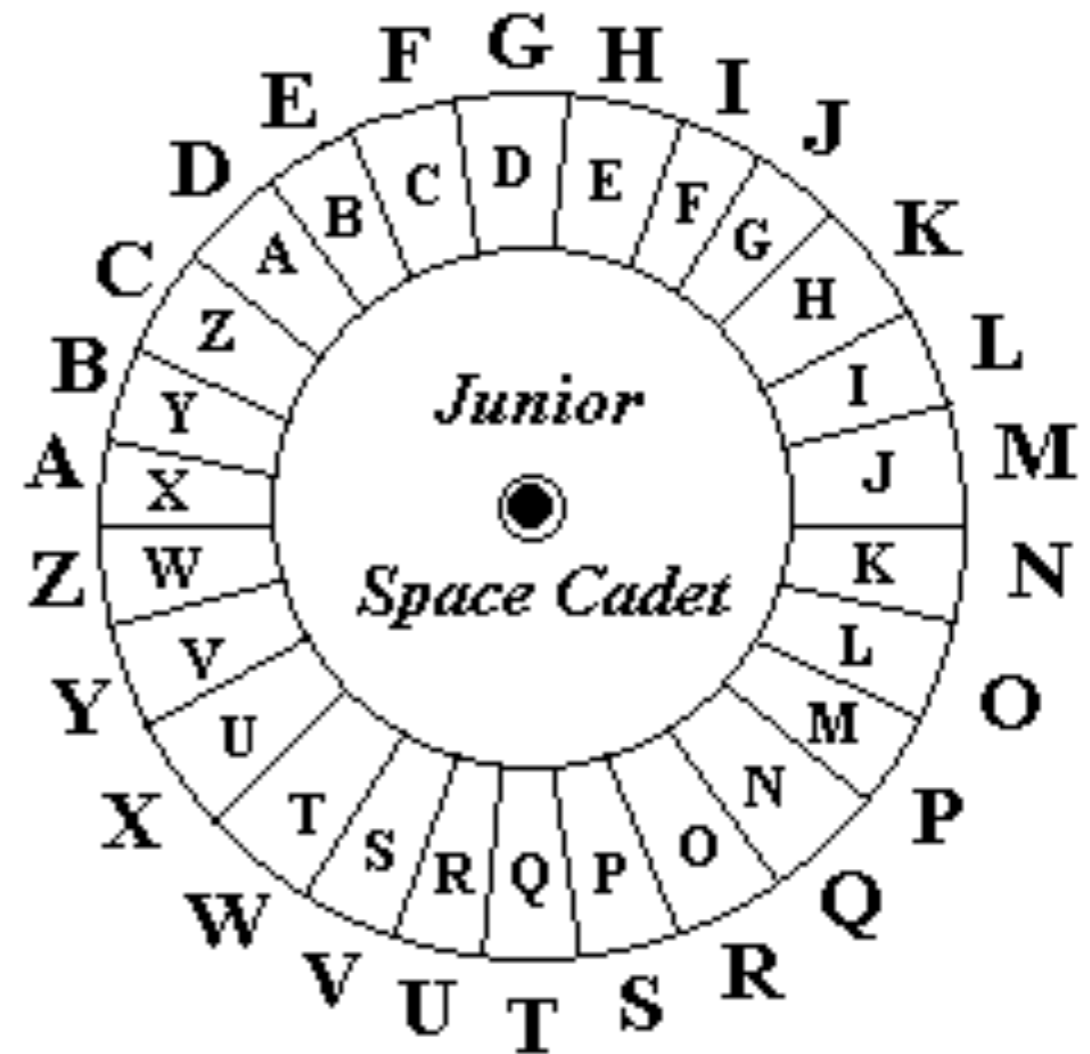


SUBSTITUTION

A SECRET MESSAGE

X PBZOBQ JBPPXDB

What's the *key*?



TRANSPOSITION

ASEC RETM ESSA GEXX

A SECRET MESSAGE

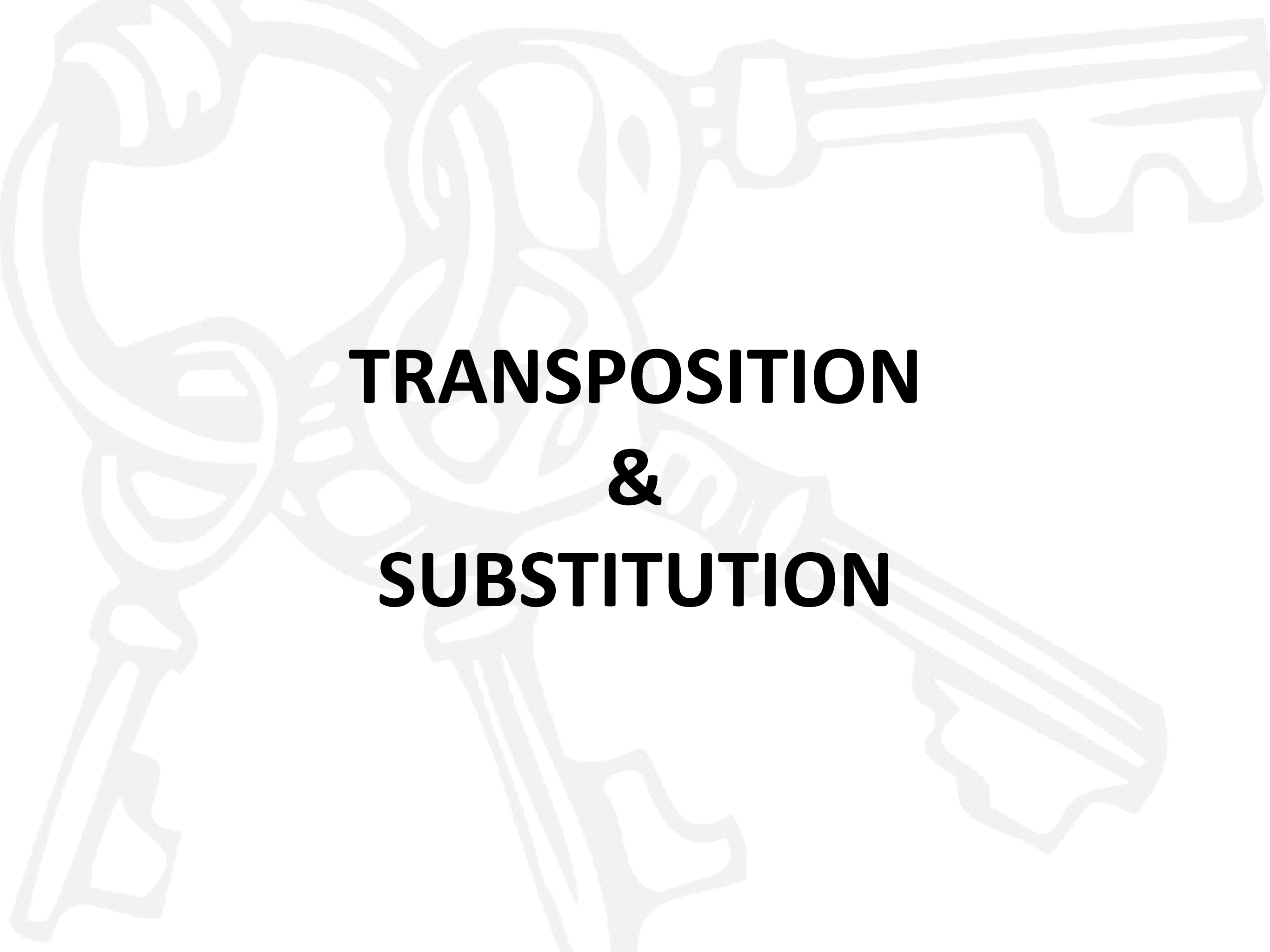
A R E G
S E S E
E T S X
C M A X

RGAE RESS TXES MXCA

R G A E
R E S S
T X E S
M X C A

What's the *key*?

RGAE RESS TXES MXCA



**TRANSPOSITION
&
SUBSTITUTION**

BITS BYTES CHARS

A SECRET MESSAGE

S is a character

8-bits byte per char

01010011

USASCII code chart

01010011					0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
0	1	2	3	4	5	6	7					
b ₄	b ₃	b ₂	b ₁	Column Row								
0	0	0	0	0	NUL	DLE	SP	0	@	P	\	p
0	0	0	1	1	SOH	DC1	!	1	A	Q	a	q
0	0	1	0	2	STX	DC2	"	2	B	R	b	r
0	0	1	1	3	ETX	DC3	#	3	C	S	c	s
0	1	0	0	4	EOT	DC4	\$	4	D	T	d	t
0	1	0	1	5	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	6	ACK	SYN	&	6	F	V	f	v
0	1	1	1	7	BEL	ETB	'	7	G	W	g	w
1	0	0	0	8	BS	CAN	(8	H	X	h	x
1	0	0	1	9	HT	EM)	9	I	Y	i	y
1	0	1	0	10	LF	SUB	*	:	J	Z	j	z
1	0	1	1	11	VT	ESC	+	;	K	[k	{
1	1	0	0	12	FF	FS	,	<	L	\	l	
1	1	0	1	13	CR	GS	-	=	M]	m	}
1	1	1	0	14	SC	RS	.	>	N	^	n	~
1	1	1	1	15	SI	US	/	?	O	_	o	DEL

AND, OR, XOR

<i>x</i>	<i>y</i>	<i>AND(x, y)</i>	<i>OR(x, y)</i>	<i>XOR(x, y)</i>
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

ONE TIME PAD

Message XOR Key = Encrypted

Length(KEY) == Length(MESSAGE)

ONE TIME PAD

Message = BUY_ | SELL | HOLD

Key = 4 random chars

Encrypted Message = XOR(M, K)

M = 1010011 1000101 1001100 1001100

K = 0110101 0100100 0011111 1010110

E = 1100110 1100001 1010011 0011010

ONE TIME PAD



Problems?

DES

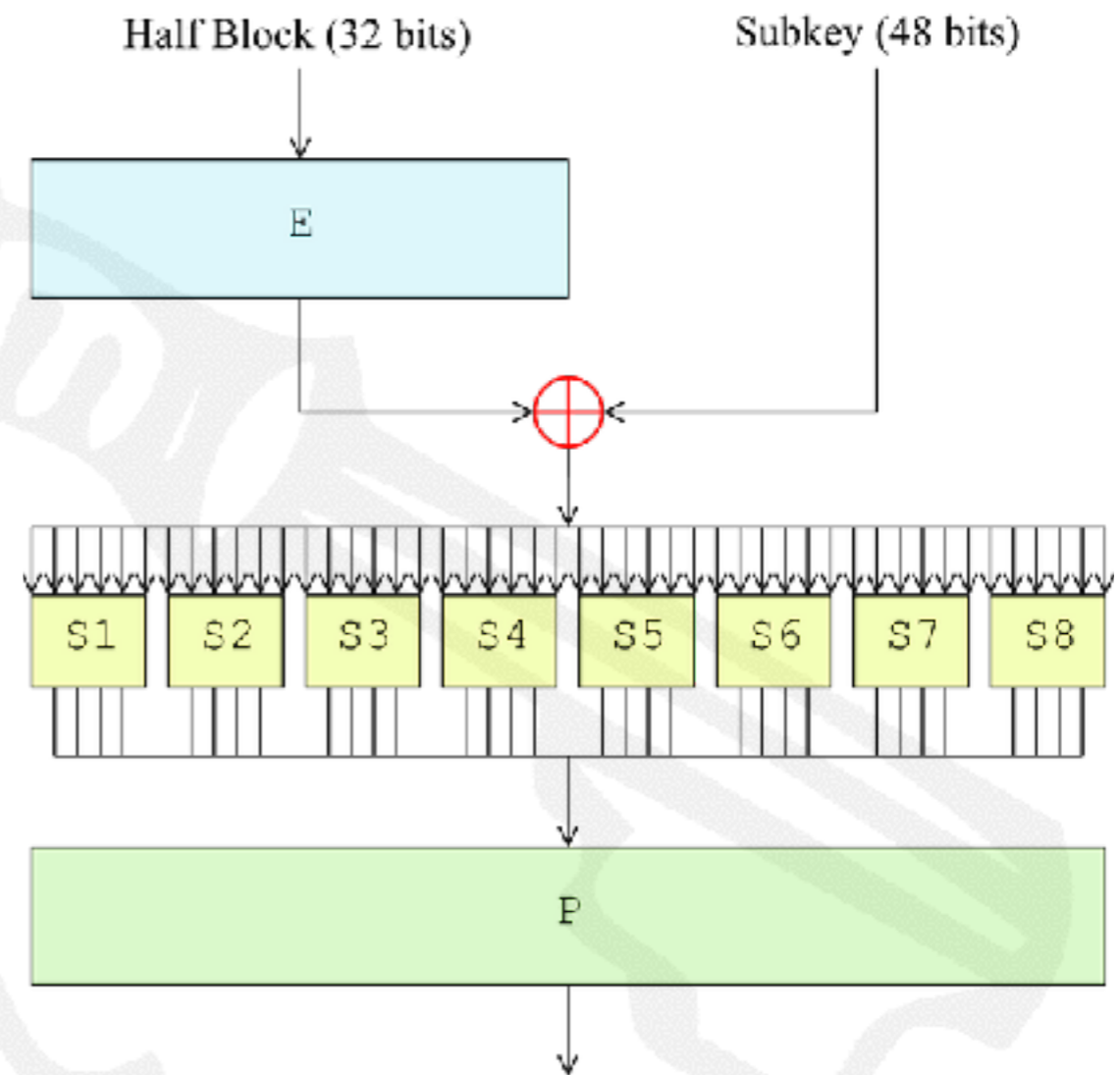
F has subs, trans, xor

Certified for gov't use:
NIST FIPS PUB 46

Tampering:

S-Boxes

Key length (64/56 bits)



DES

What's the *key*?

(64-bits => 56-bits + 8 parity bits)

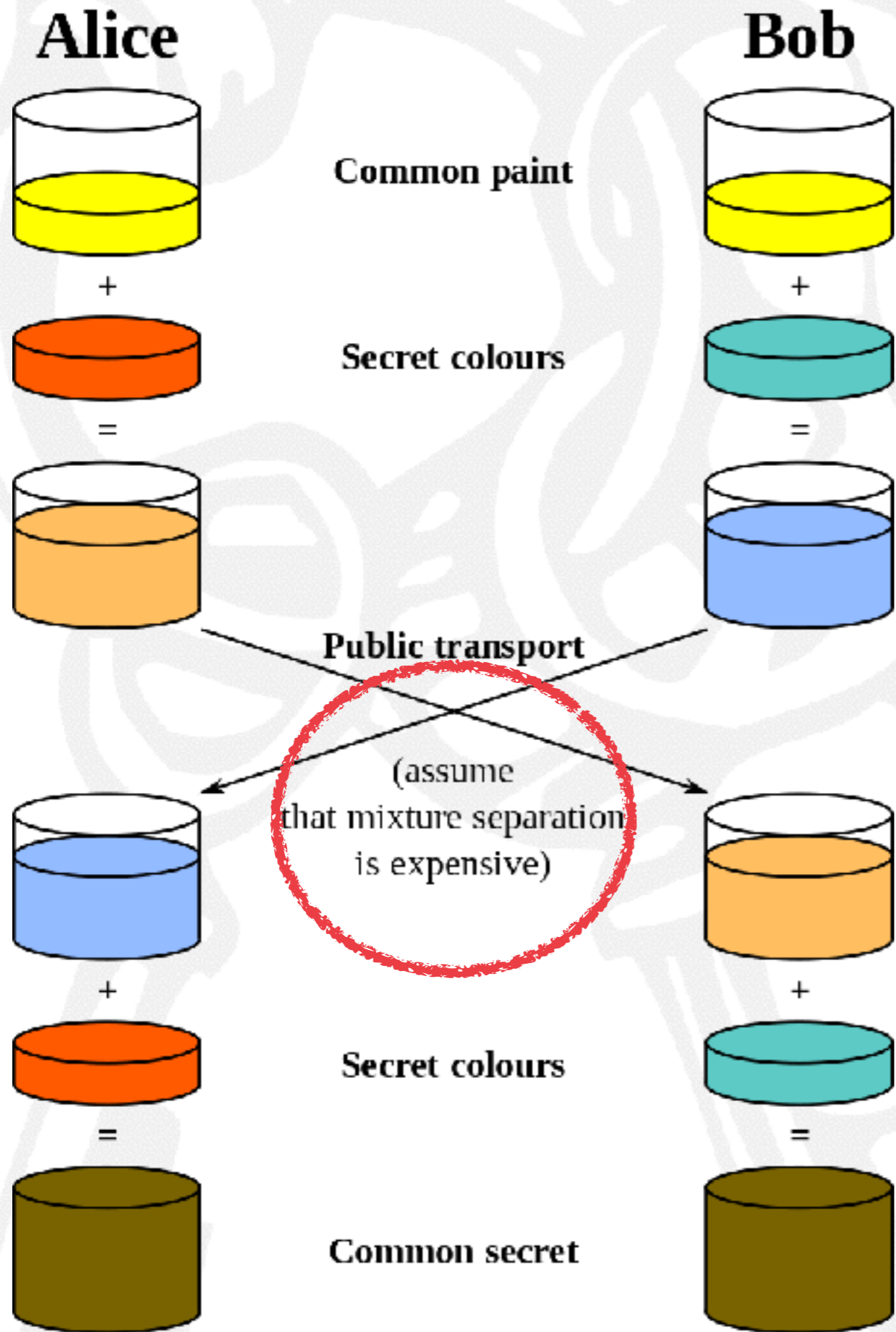
Problems?

AES: *Stick Figure Guide*

DIFFIE HELLMAN KX

Key exchange

Solve the key-sharing problem



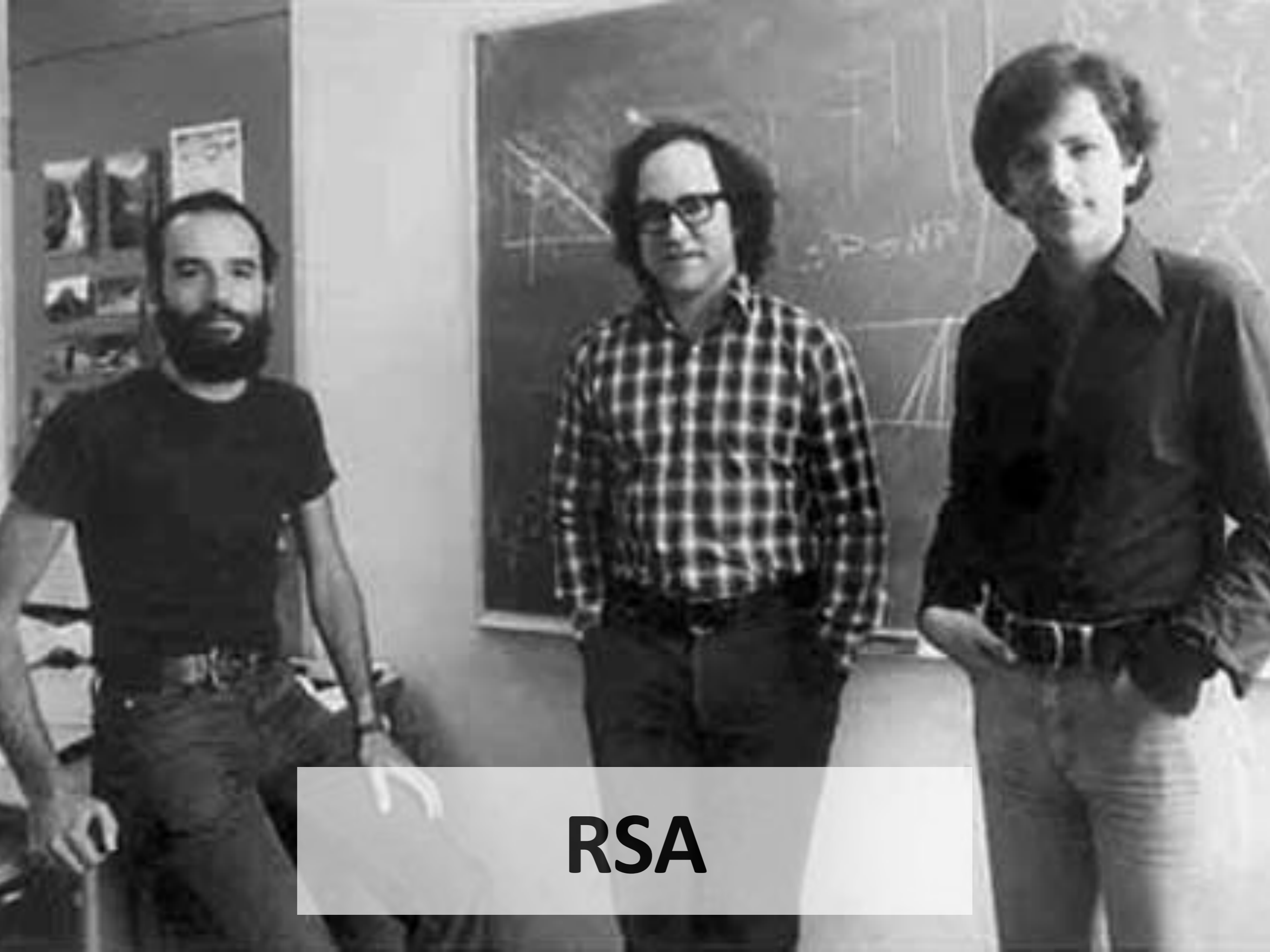
Crypto Characters:

Alice & Bob

Eve (passive adversary)

Mallory (active adversary)

I like the cookie-dough version of this...



RSA

RSA

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.15 (Darwin)

Asymmetric System

Public Key

Private Key

A “hard” problem:
factoring large #s

```
mQENBFJzvH8BCAC4PUtwEeeaa6SescpfbJ+ENbwkcc/hdEjId7/nzSqgm/JX2KN7
2XYrjoSByGa6VnwGZEeq4A0Yepbrn6oNANyYqVcp90WlJmB2Ij65v9YxVv27PGtbe
9TCAzeD20+1CMJcp7BjX46dF6sS9CjV8KB2aIcuTTh/qCTGpxmcAdDM8A3+Zy0X2
TngHz8EGVaeK1qjmrGS16b6nF0oKYILLXylrgnpuoYp0oQrCuLzY1eaX90p2r2W2
hdATbb7Z7bTXgvgfPZSYI1pbpPrbZQCQCqSz7y9IHDcA3nztTNrcRg60/6+4tF0P
mJqspXlCjQsW6ekbfEMwf2QITTheEYtcA9CbABEBAAG0IkRhbml1bCBNZWRpbmEg
PG1lZGluYUBtb25nb2RiLmNvbT6JATgEEwECACIFAlJzvH8CGwMGCwkIBwMCBhUI
AgkKCwQWAgMBAh4BAheAAAoJEM1ISIrK5R5MiMIAJiAIX2Ase1LgtVXmqdEis9W
AphM09A8/vFCBIwtauL7QTnhXqcaxnZ6VMrpRbOCtSHRWV6q6NUdJ5ZG7GQV9/05
DT8yEuUp5Rqt0zMc1d+h58PlzaCV54NNvx2LUtK+0XrLr7Gb6GHjUZGLK0g2gGlg
T67CeYcEtNQMEEEuOgp0/gxM72mF1N66lt4GT5X60YwJRNyTXDA67WzRiMlpbwB0
k9LX3lttzm2TpR1GAZ3Z/VFi+ZJPFqj1P+vS0ibKsYtb3xAdf3x5zfthRqSQ0SjH
1ji3F8zV03jFR6Acfvgw8XH0pi0cRve+Z6TuJKV6ZrJQaREDo0v1DwhSPVXa5uG5
AQ0EUn08fwEIANmz2yQ1fMuKJm++s/bo+TwUcgVbwq7bzkJIw81bX81v1l0qEt4x
We6oThIqW647fqcK6aw3W9gHccspIbd56QAGRfuaML11EYNNZZaHEjhuqOrKnN+D
19mi077uzQy1ff/dT5fSCySfNAiPCTljlzxsu6P/o73rvbXxkAzhUjz9/nlBqUjc
P7MU+nEGaPYG0poNok+XeOd/A9MGtjlqQq8GclnJKYiWe6MKAWZiNzC9A0mLSXRj
at/qiWYG90LJ9a/xJnjEdP519mZF0SG2ZSe+vMqisqw0i0KV5//OXohxPdonfIvM
t96aWlf7a0btcpnGyQgoKnvqVBC1N6SWcPEAEQEAAAYkBHwQYAQIACQUcUn08fwIb
DAAKCRDNSEiK5CuUeV4vB/9gkePoPVD3Go0ZTI9k1uyUi7FuxLkdP1NqaL6M1hmq
45k/LFxmcN8Cr5bULrdHY82QtHke3wQFKWz0V0aCS14B0Gi+v2VjYh1Qo5nE0BnA
Yibm3BK//yd0WI5HsJ4nZkvwmPLHsEx4q00E9lms9tFyJmmdYroy5m4yldvG+app
1vHZ0sJSRz1oCG0aQzmHwPyNXxNBCN4RnP9ib2KGI4Nvqq92/IY7YLNmX0gmsvNL
o2g3whjeyRCuYqF41v7GZscy+K1QE1BzVrVrBIX8y2pRPM/Pcie0Ie0JSZzF4w3V
/aFY9r9rA9ARYHHucamc7dezr6t0EQ3lz/yFRvtL5pJR
=qKYQ
```

-----END PGP PUBLIC KEY BLOCK-----

HASH FUNCTIONS

MD5: 128 bits, `md5` or `openssl md5`

'I leave all my fortune to Alice' | md5

19755c81218340ed42f575bff3691c57

'I leave all my fortune to Bob' | md5

4b67189b91f32b8a12f968ea1989a8fe

This would be bad

'I leave all my vast fortune to Eve' | md5

19755c81218340ed42f575bff3691c57

HASH FUNCTIONS

SHA1: 160 bits, `shasum` or `openssl sha1`

```
echo 'Hello, World' | shasum -a 1 # 160 bits  
4ab299c8ad6ed14f31923dd94f8b5f5cb89dfb54
```

```
echo 'Hello, World' | shasum -a 256 # 256 bits  
8663bab6d124806b9727f89bb4ab9db4cbcc3862 \  
f6bbf22024dfa7212aa4ab7d
```

```
echo 'Hello, World' | shasum -a 512 # 512 bits  
44c4f73161332b2b058360310640c6704796ece7 \  
6593e22ca32f76ccbc2c469d5b26ae64b996c781 \  
65929ac1af7f9a0ae6132010c917f6b104196b86 \  
48e108d3
```

HYBRIDS

We know about:

Symmetric Key Encryption

Asymmetric Key Encryption

Key Exchange

Hash Functions

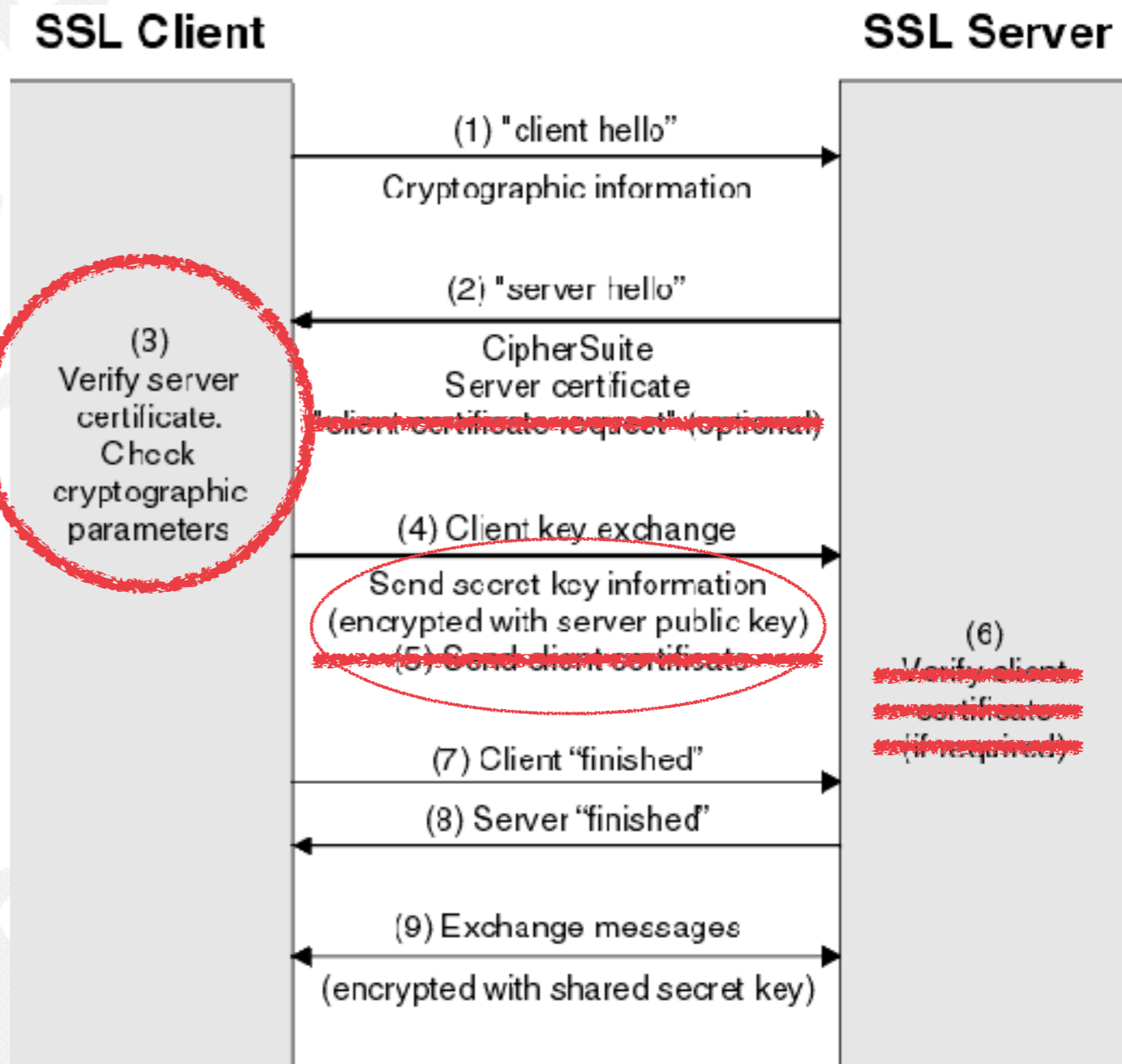
How to mix and match?

SSL / TLS

Confidentiality
Integrity
Authenticity

“Data in transit”
security on the Internet

Increasingly attacked





China Internet Network Information Center EV Certificates Root

Root certificate authority

Expires: Saturday, August 31, 2030 at 3:11:25 AM Eastern Daylight Time

✔ This certificate is valid

Name	Kind	Expires	Keychain
Autoridad de Certific...aiz del Estado Venezolano	certificate	Dec 17, 2030, 6:59:59 PM	System Roots
Baltimore CyberTrust Root	certificate	May 12, 2025, 7:59:00 PM	System Roots
Belgium			System Roots
Buypass			System Roots
Buypass			System Roots
Buypass			System Roots
Buypass			System Roots
CA Disig			System Roots
CA Disig			System Roots
CA Disig			System Roots
Certigna			System Roots
Certinon			System Roots
certSIGN			System Roots
Certum C			System Roots
Certum T			System Roots
Chambe			System Roots
Chambe			System Roots
China In			System Roots
Cisco Ro			System Roots
Class 1 F			System Roots
Class 1 F			System Roots
Class 1 F			System Roots
Class 2 F			System Roots
Class 2 F			System Roots
Class 2 F			System Roots
Class 2 F			System Roots
Class 2 F			System Roots
Class 3 Public Primary Certification Authority	certificate	Aug 1, 2028, 7:59:59 PM	System Roots
Class 3 Public Primary Certification Authority	certificate	Aug 2, 2028, 7:59:59 PM	System Roots
Class 3 Public Primar...ertification Authority - G2	certificate	Aug 1, 2028, 7:59:59 PM	System Roots
Class 4 Public Primar...ertification Authority - G2	certificate	Aug 1, 2028, 7:59:59 PM	System Roots
CNNIC ROOT	certificate	Apr 16, 2027, 3:09:14 AM	System Roots
Common Policy	certificate	Oct 15, 2027, 12:08:00 PM	System Roots
COMODO Certification Authority	certificate	Dec 31, 2029, 6:59:59 PM	System Roots

China Internet Network Information Center EV Certificates Root
 Root certificate authority
 Expires: Saturday, August 31, 2030 at 3:11:25 AM Eastern Daylight Time
 ✔ This certificate is valid

▶ Trust
 ▼ Details

Subject Name

Country CN
 Organization China Internet Network Information Center
 Common Name China Internet Network Information Center EV Certificates Root

Issuer Name

Country CN
 Organization China Internet Network Information Center
 Common Name China Internet Network Information Center EV Certificates Root

Serial Number 1218379777
 Version 3

Signature Algorithm SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
 Parameters none



home.nyu.edu

Identity verified

Permissions

Connection



The identity of this website has been verified by InCommon Server CA.

[Certificate Information](#)



Your connection to home.nyu.edu is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using RC4_128, with MD5 for message authentication and RSA as the key exchange mechanism.

The server does not support the TLS renegotiation extension.



Site information

You first visited this site on Nov 21, 2013.

[What do these mean?](#)



Academics Work Research News

Alerts +

Downloading
"late"
in alert"
"ACCOUNT" Phishing Scam
against Acrobat, PDF Reader

+
contains name, address,
information for NYU faculty,

Help, FAQs, Contact ITS

Need help using NYUHome? Ask a Question, comment, feed

Lists

NYU Lists, also called *Lyrn*, allow students to exchange ideas, confirm meeting changes, subscribe, follow the "Bro

Current Subscription

Issuer Name	
Country	US
Organization	Internet2
Organizational Unit	InCommon
Common Name	InCommon Server CA
Serial Number	38 9E 22 ED 6F 23 02 F2 F3 4E 58 D8 BC 57 FD BC
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Thursday, January 10, 2013 at 7:00:00 PM Eastern Standard Time
Not Valid After	Monday, January 11, 2016 at 6:59:59 PM Eastern Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : B0 CE 28 14 3F BE F8 D0 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	256 bytes : 4A 6D AD 29 2D C7 42 87 ...
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Digital Signature, Key Encipherment

AddTrust External CA Root
InCommon Server CA
home.nyu.edu

home.nyu.edu

Issued by: InCommon Server CA

Expires: Monday, January 11, 2016 at 6:59:59 PM Eastern Standard Time

✔ This certificate is valid

Details

Subject Name	
Country	US
Postal Code	10003
State/Province	NY
Locality	New York
Street Address	10 Astor Place
Organization	New York University
Organizational Unit	ITS eServices
Common Name	home.nyu.edu
Issuer Name	
Country	US
Organization	Internet2
Organizational Unit	InCommon
Common Name	InCommon Server CA

Fingerprints

SHA1	97 DF 17 0E 49 E9 9A B2 20 65 49 BB 6F BA 18 56 D4 6B 70 BA
MD5	A0 F4 B0 83 A1 25 51 BA 40 F6 FC EC D6 33 8B 72

Twitter, Inc.

Identity verified

Permissions

Connection



The identity of Twitter, Inc. at San Francisco, California US has been verified by VeriSign Class 3 Extended Validation SSL CA.

[Certificate Information](#)



Your connection to twitter.com is encrypted with 128-bit encryption.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.



Site information

You first visited this site on Nov 15, 2013.

[What do these mean?](#)

Home to Twitter.

Conversation, explore your interests, and be in the know.





www.mongodb.com

This site uses a weak security configuration (SHA-1 signatures), so your connection may not be private.

Permissions

Connection



The identity of this website has been verified by Gandi Standard SSL CA. No Certificate Transparency information was supplied by the server.

The certificate chain for this website contains at least one certificate that was signed using a deprecated signature algorithm based on SHA-1.

[Certificate Information](#)



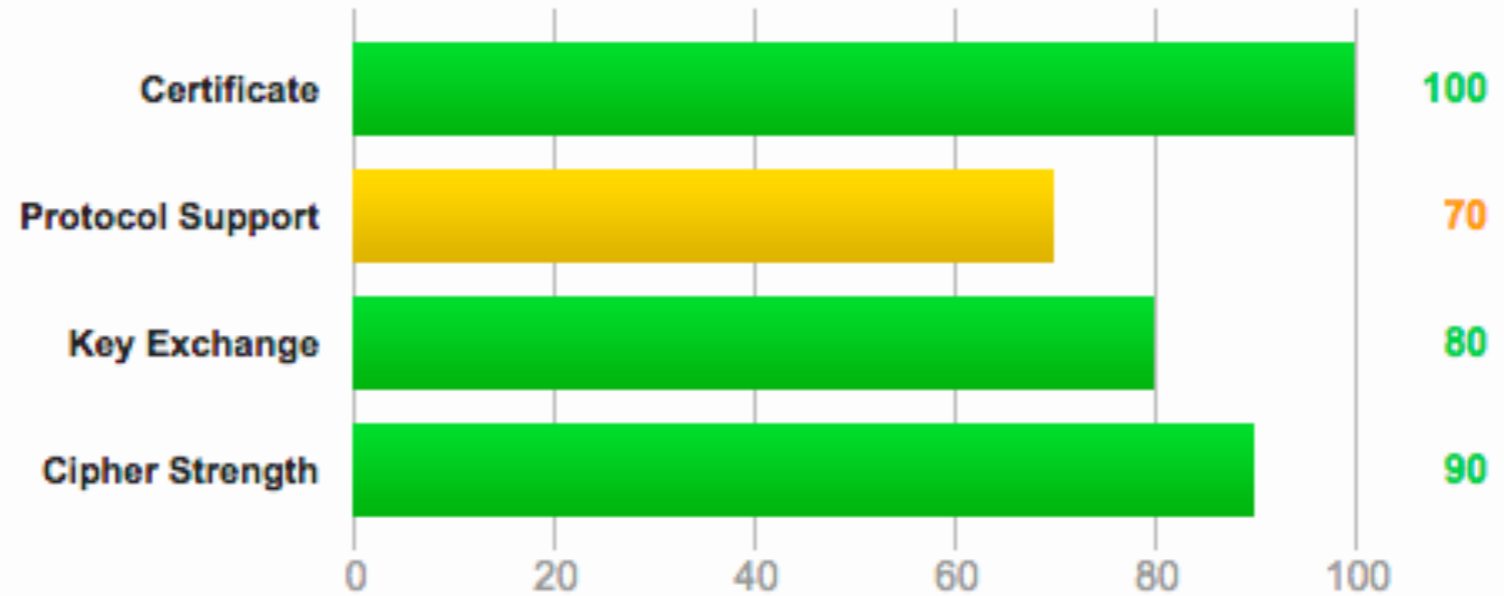
Your connection to www.mongodb.com is encrypted using an obsolete cipher suite.

The connection uses TLS 1.2.

The connection is encrypted using AES_128_CBC, with HMAC-SHA1 for message authentication and DHE_RSA as the key exchange mechanism.

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. [MORE INFO »](#)

Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

SSL / TLS

Lots of background readings on the challenges

- *Heartbleed, comic* (SSL/TLS vulnerability)
- *Attacks on SSL* (iSec Partners)
- *SSL Observatory* (EFF)
- *The most dangerous code in the world*
- *SSL Labs / SSL Labs Grading Changes January 2017*
- Rogue CAs: *faking google.com, getting hacked, and generally failing*

TOOLS

- openssl command-line tools for almost all ciphers, hashes, and combinations
- Small exercise with openssl encryption modes
- SSL Labs provides excellent “scoring”
- SSL Checker decode certificates
- Let’s Encrypt is a free CA that works with web servers to generate certificates
- Keybase is public / private key hosting for people

OTHER CRYPTO READINGS

- *Crypto 101*, online book under development
- *Security Engineering*, Ross Anderson
- *The Debian PRNG Bug*, HD Moore (2008)
- *Randomness and the Netscape Browser* (1996)
- *Windows NT rantings from the L0pht* (1997)
- *Encrypting the Web*, EFF

NSA, CIA, OTHER TLAS

That capability [of the NSA and US intelligence community] at any time could be turned around on the American people and no American would have any privacy left. There would be no place to hide.

If this government ever became a tyranny, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny. There would be no way to fight back, because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capacity of this technology.

*I don't want to see this country ever go across the bridge. I know the capacity that is there to make tyranny total in America, and **we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision so that we never cross over that abyss.** That is the abyss from which there is no return*

Sen. Frank Church, 1975, a quote I know from *Decrypting the Puzzle Palace*
I used to call this the "scary quote". Now it's current events.

