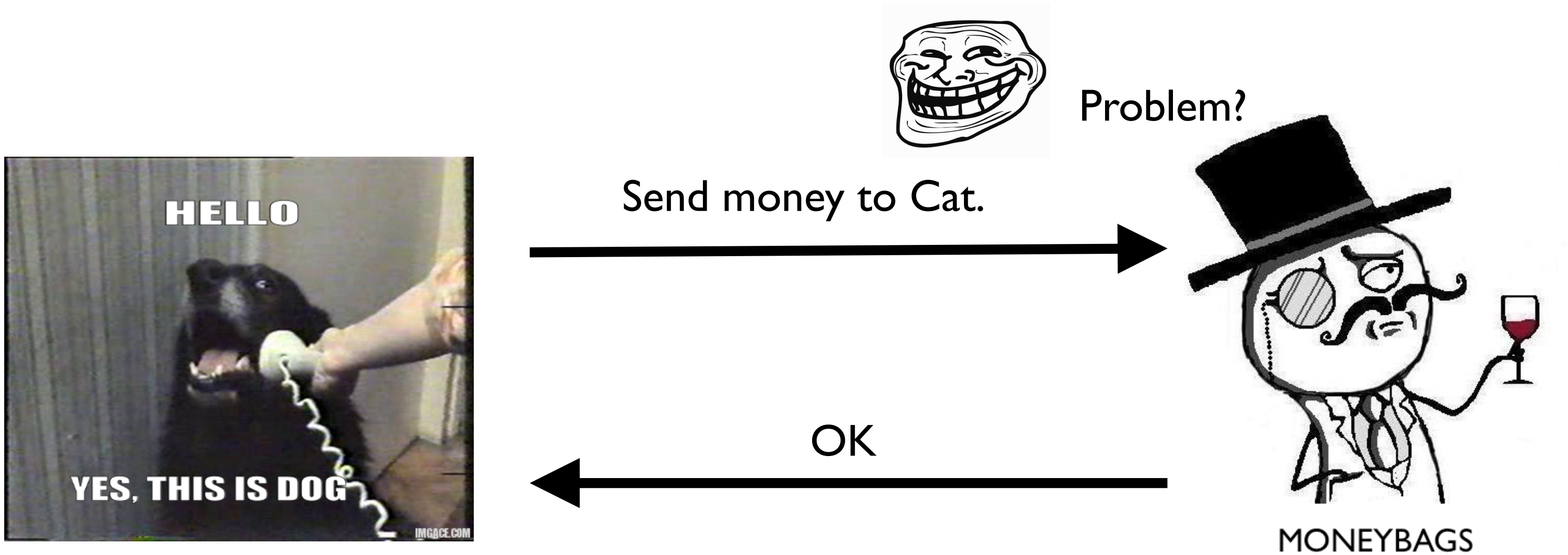
Cryptography and Cryptanalysis

By Huw

Basic Communication



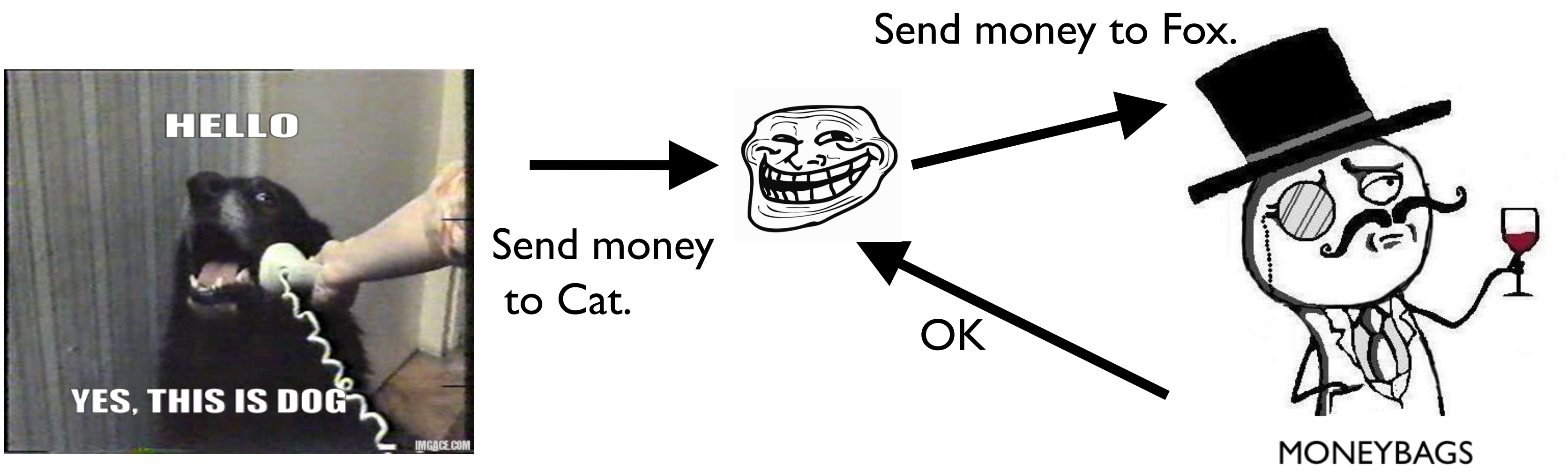
Problem?

Send money to Cat.

OK

MONEYBAGS

Problem?



Send money to Cat.

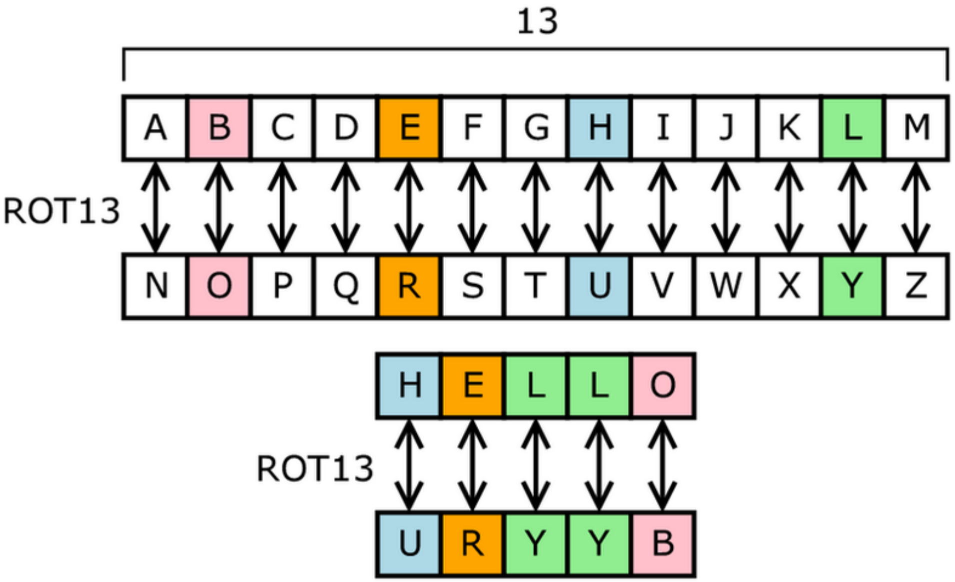
Send money to Fox.

OK

MONEYBAGS

Encypher!

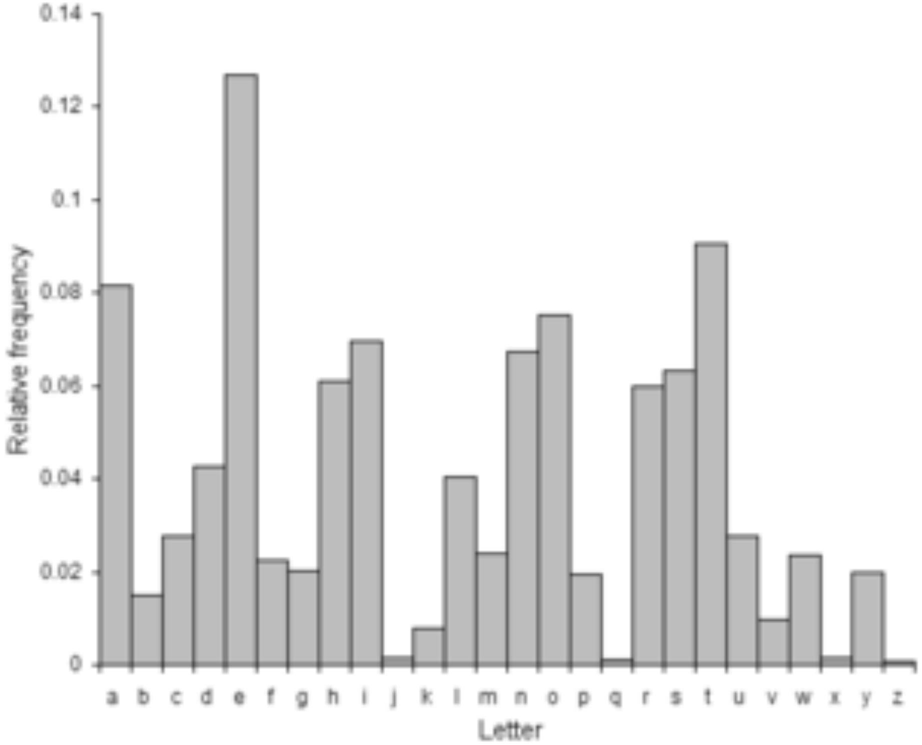
- Algorithm 1:
  - Replace every letter by another in the alphabet. (Caeser cypher):



```
plain:  HELLO THIS IS DOG
cypher: URYYB GUVF VF QBT
```

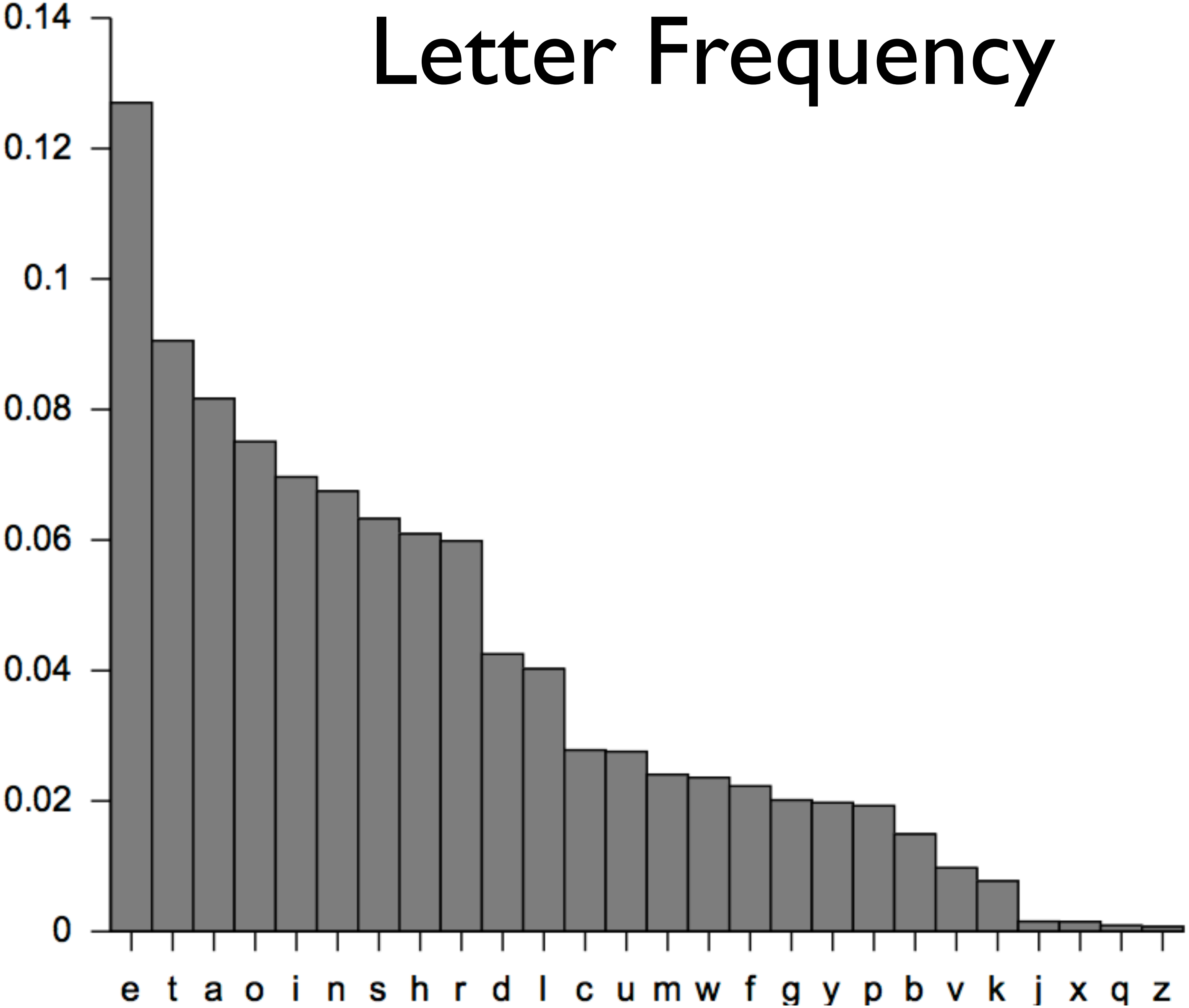
Encypher!

- Algorithm 1:
  - Obvious problem!
  - Very unsuitable for very much data.
  - Can ‘brute force’



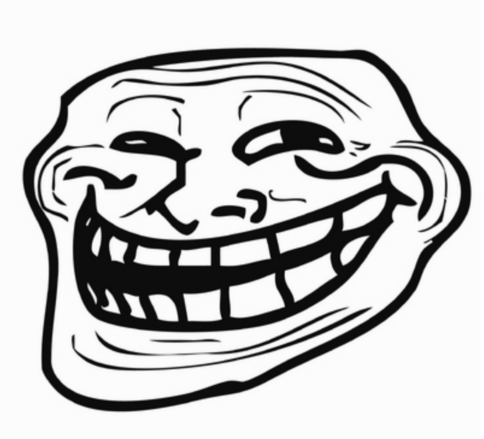
```
plain:  HELLO THIS IS DOG
cypher: URYYB GUVF VF QBT
```

Letter Frequency



:(

- We have to assume that the bad guy knows the method we're using to encypher our text.



- This is where a KEY comes in
  - useful for varying our algorithm slightly each time.

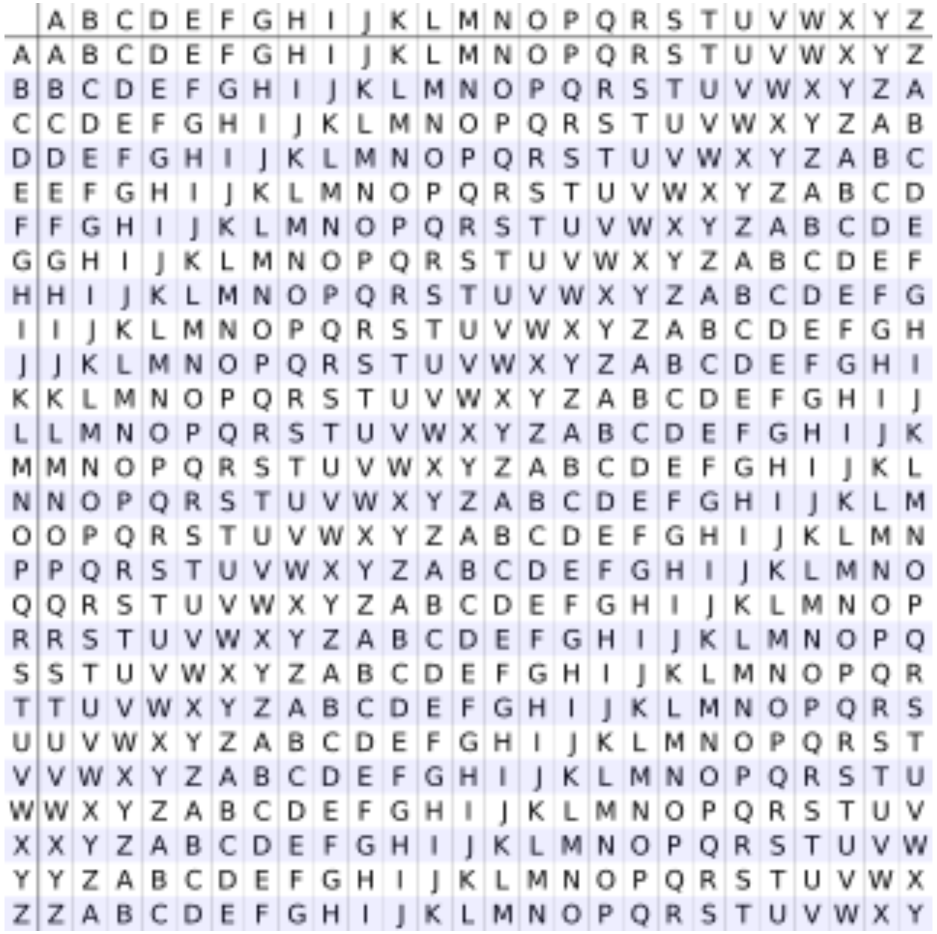
Polyalphabetic Cipher

- Algorithm 2:
  - Change the substitution alphabet for every letter.
  - Change by how? That's determined by the key.

```
key:    DOGDO GDOG DO GDO
plain:  HELLO THIS IS DOG
cypher: KSROC ZKWY LG JRU
```

Polyalphabetic Cypher

- row = key
- col = plain
- cypher = (row, col)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

```
key:    DOGDO GDOG DO GDO
plain:  HELLO THIS IS DOG
cypher: KSROC ZKWY LG JRU
```

UNBREAKABLE Cypher

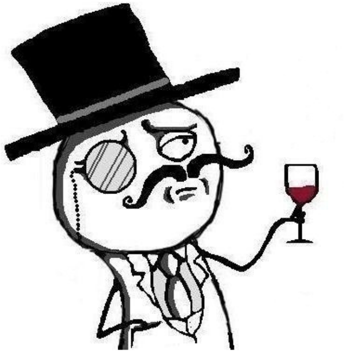
- Actually very easy…
- Just make the key the same size as the plain text (only ever use the key once!)
- Easy!
  - Except the key is the same size as the plain text and can only ever be used once…

```
key:    DJFDS SFFD AD POL
plain:  HELLO THIS IS DOG
cypher: KNQOG LMNV IV SCR
```

Simple Encryption

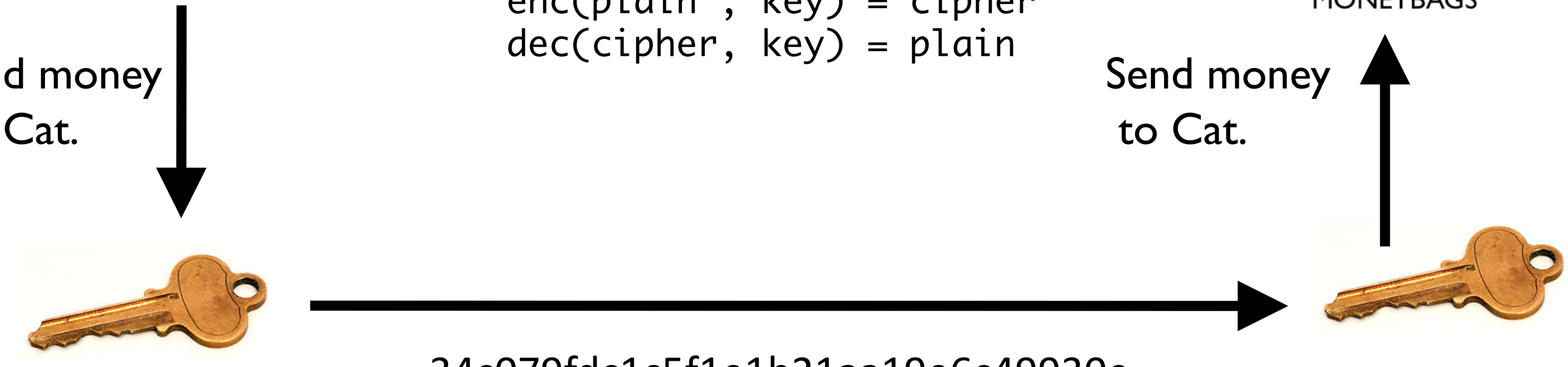
In reality, there's some much better algorithms. All follow that basic principal:

```
enc(plain , key) = cipher
dec(cipher, key) = plain
```



MONEYBAGS

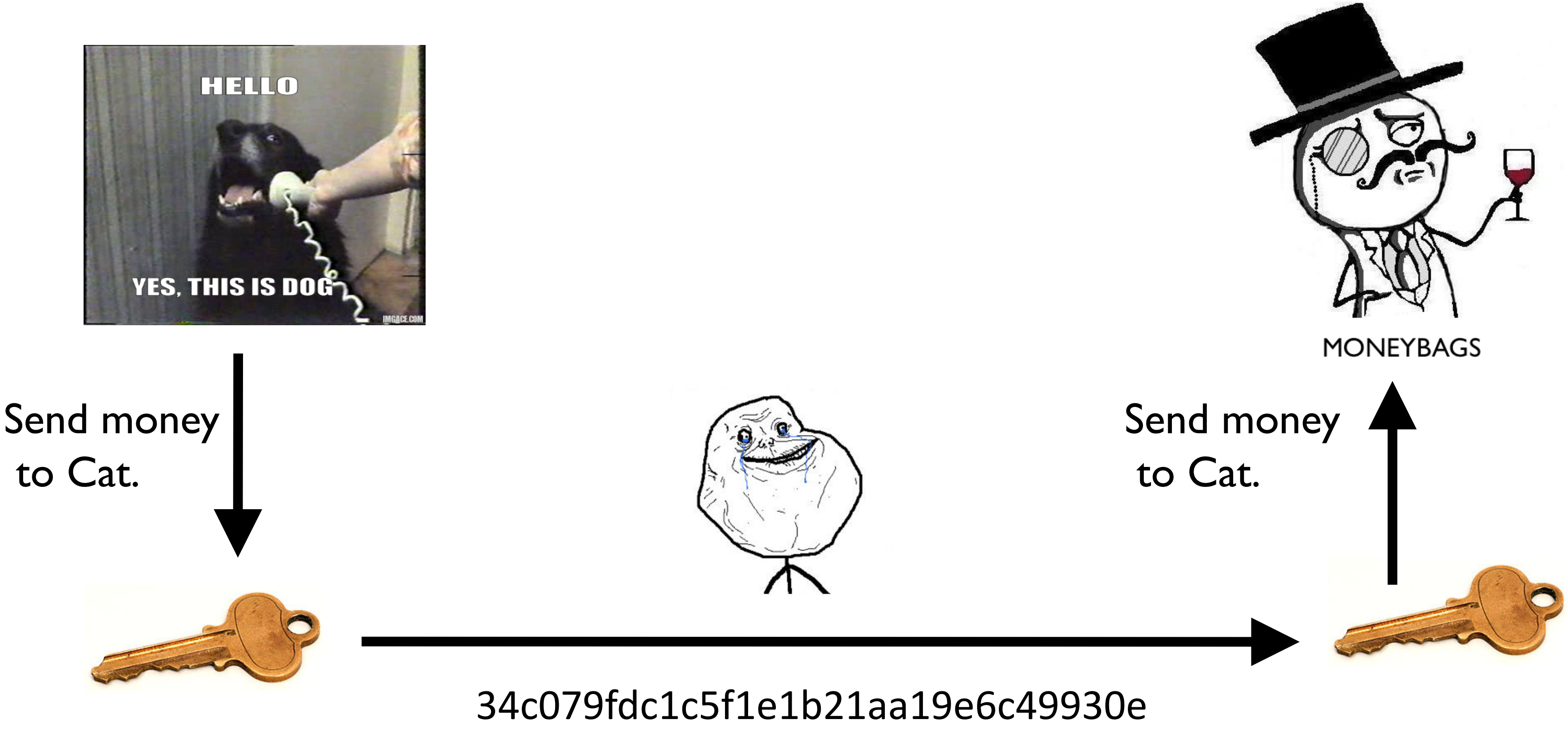
Send money to Cat.



Send money to Cat.

34c079fdc1c5f1e1b21aa19e6c49930e

Simple Encryption



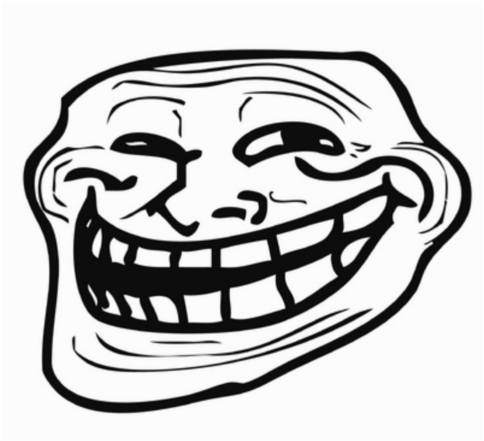
Send money
to Cat.

MONEYBAGS

Send money
to Cat.

34c079fdc1c5f1e1b21aa19e6c49930e

BUT



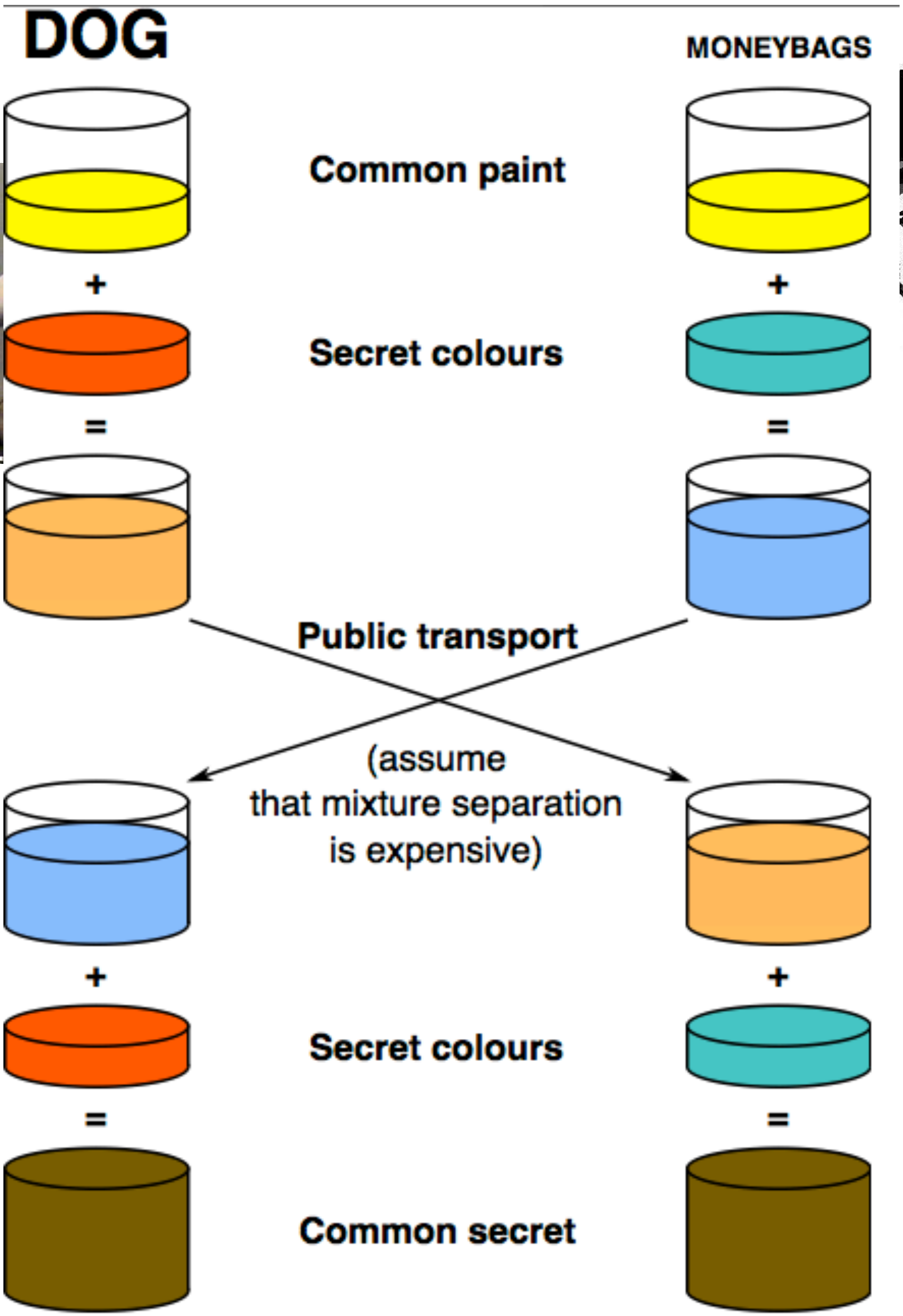
How should Dog and Mr Moneybags agree on a key?

Key distribution

- They could meet together somewhere private?
- They could just hope no one is eavesdropping?
- They could use some funky mathematics?

- They just talk to their friends:

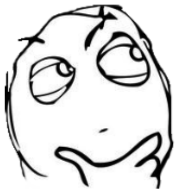
Diffie and Hellman



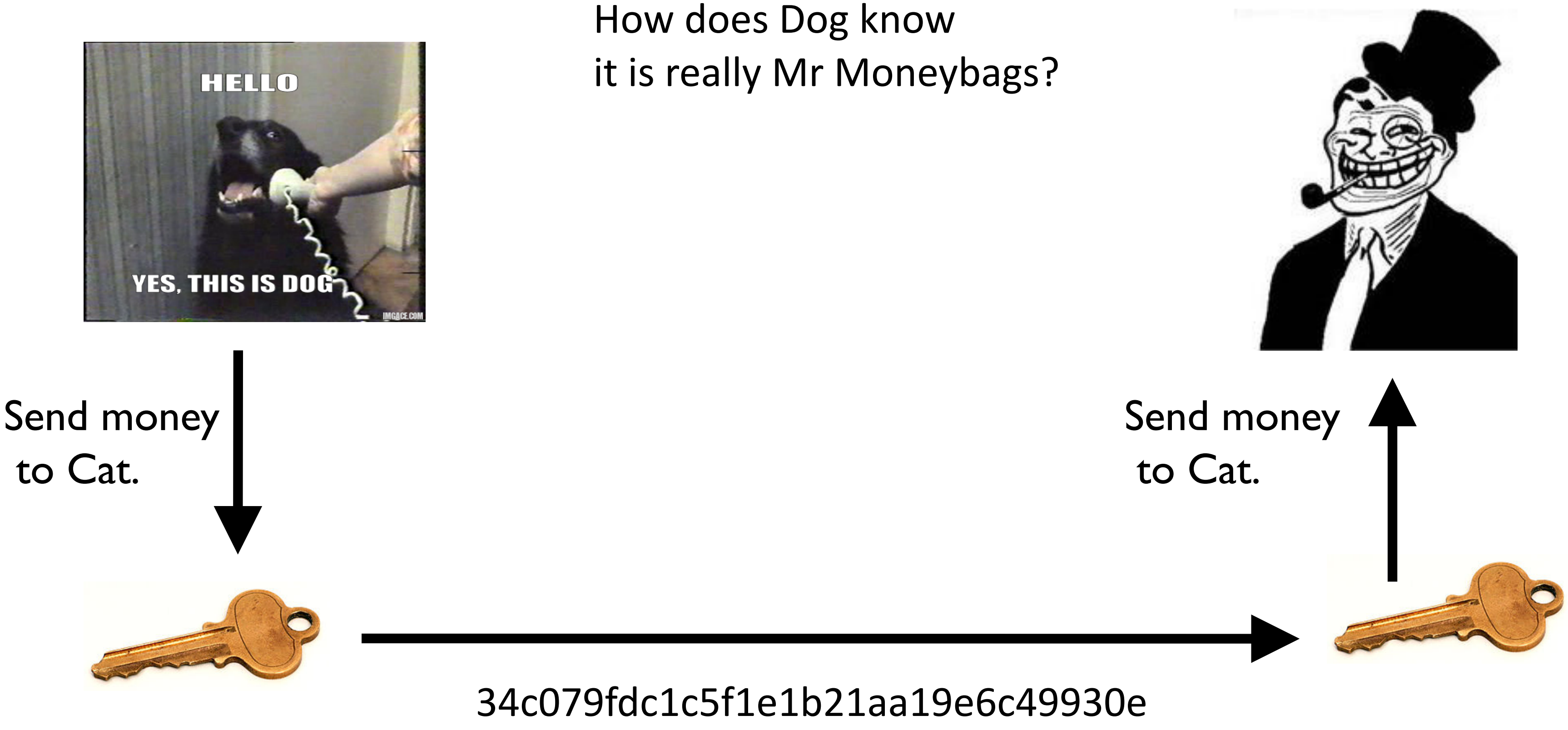
MONEYBAGS

No one eavesdropping is able to guess the secret colour!

Except they are actually using huge prime numbers rather than paint…



HOWEVER…



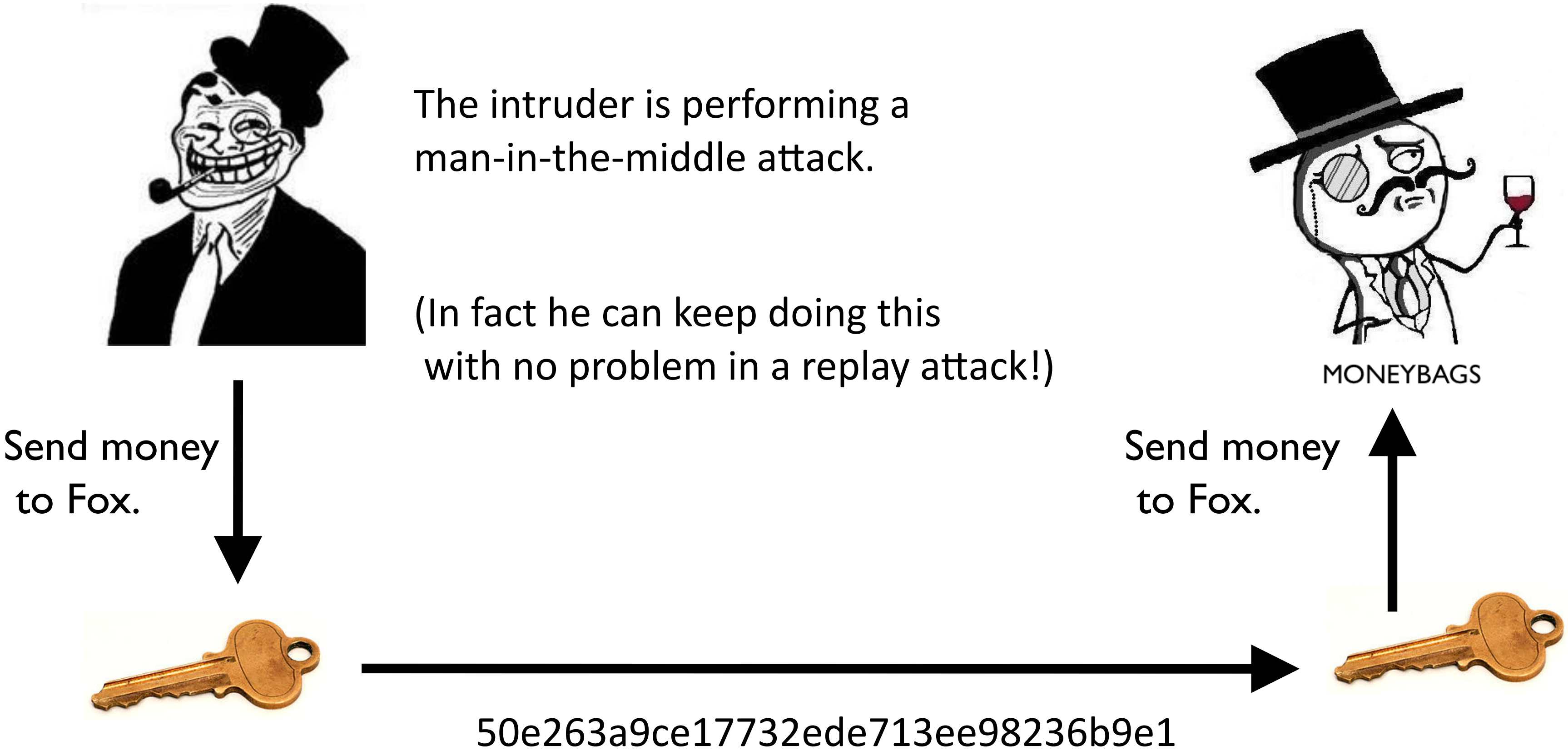
How does Dog know
it is really Mr Moneybags?

Send money
to Cat.

Send money
to Cat.

34c079fdc1c5f1e1b21aa19e6c49930e

AND NOW!



The intruder is performing a man-in-the-middle attack.

(In fact he can keep doing this with no problem in a replay attack!)

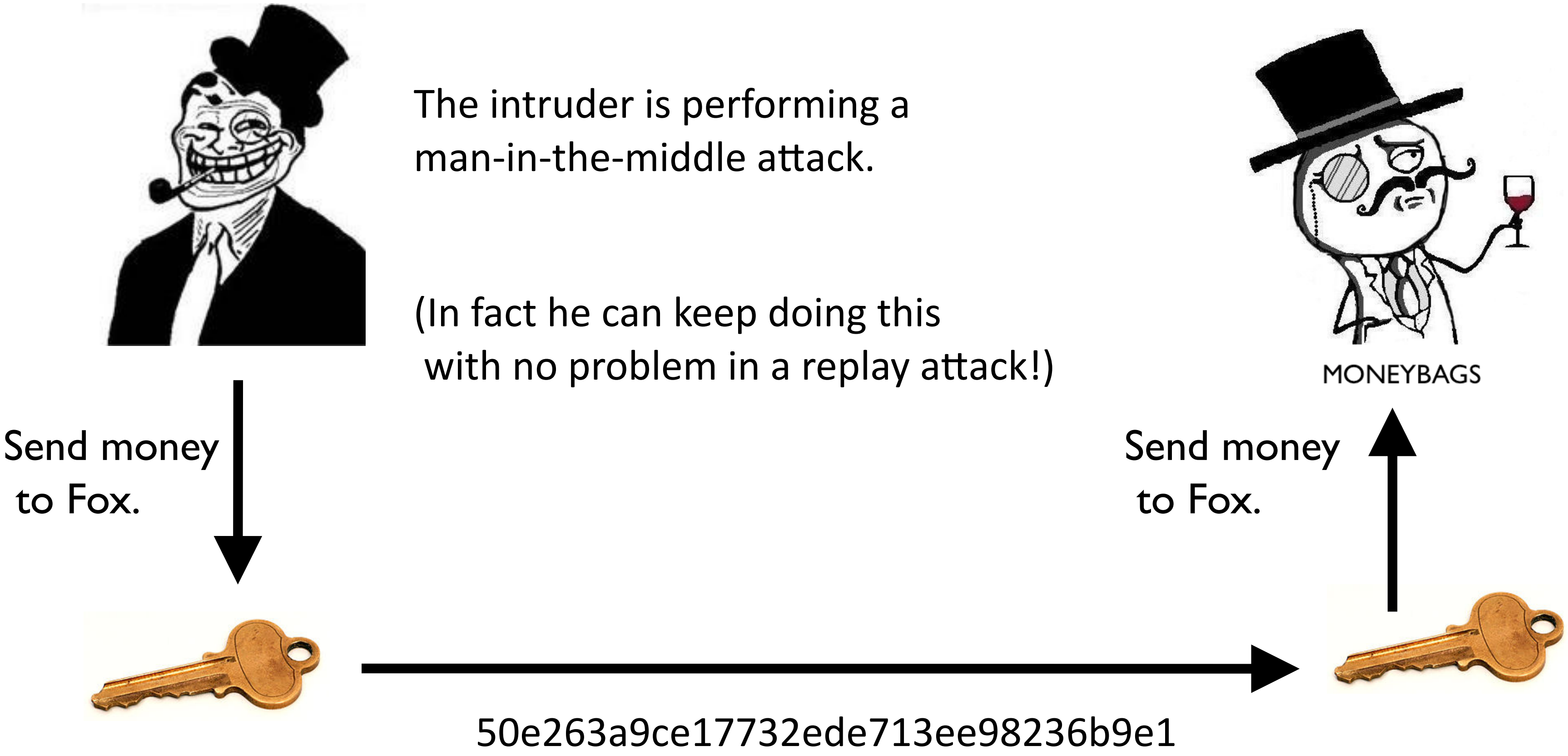
MONEYBAGS

Send money to Fox.

Send money to Fox.

50e263a9ce17732ede713ee98236b9e1

AND NOW!



The intruder is performing a man-in-the-middle attack.

(In fact he can keep doing this with no problem in a replay attack!)

MONEYBAGS

Send money to Fox.

Send money to Fox.

50e263a9ce17732ede713ee98236b9e1

References

The best textbook on Computer Networks:

- Tanenbaum, Andrew S., 1989 *Computer networks / Andrew S. Tanenbaum* Prentice-Hall, Englewood Cliffs, N.J.

The best textbook on Algorithms, (including Diffie Hellman):

- T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, 2009 *Introduction to Algorithms* MIT Press, 3rd Edition

Also: Wikipedia has a good intro to the Diffie-Hellman exchange:

http://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange