Anamorphic-Resistant Encryption

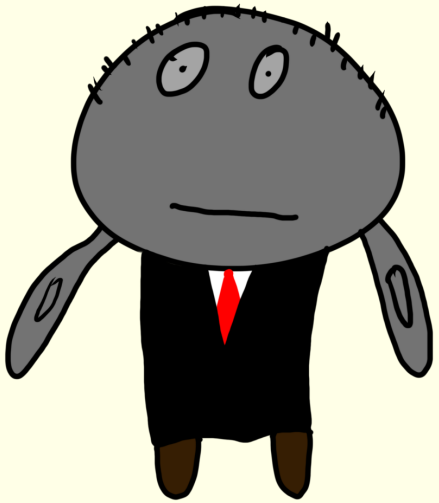
Or, why the encryption debate is still alive

Yevgeniy Dodis, **Eli Goldin**

Encryption Debate

Privacy Advocate

Mr. Government

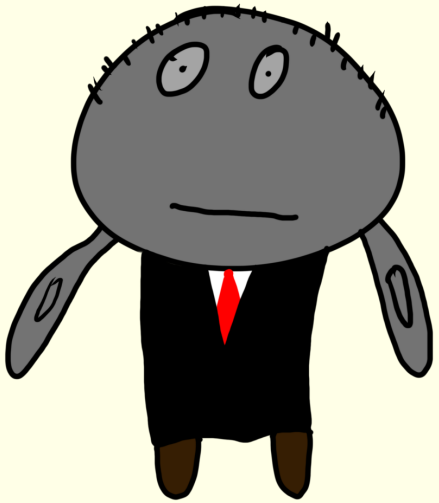


Encryption Debate

Privacy Advocate

- Everything should be encrypted

Mr. Government



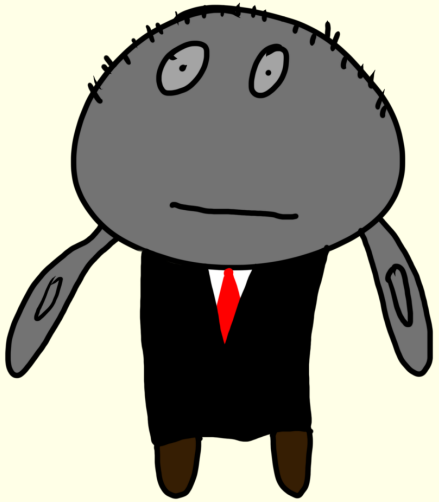
Encryption Debate

Privacy Advocate

- Everything should be encrypted

As long as I can read it.

Mr. Government



Encryption Debate

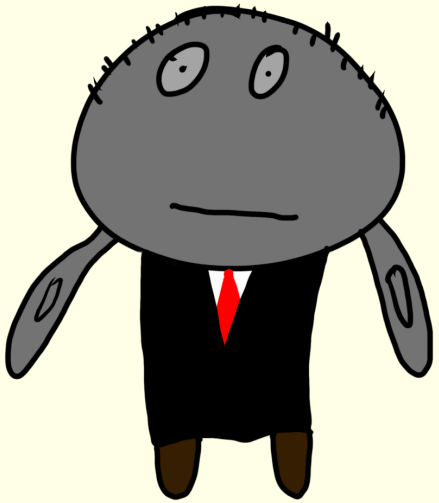
Privacy Advocate

Everything should be encrypted

As long as I can read it.

Add backdoor?

Mr. Government



Encryption Debate

Privacy Advocate

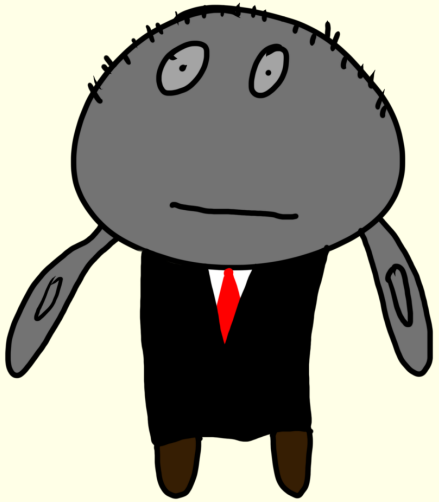
- Everything should be encrypted

As long as I can read it.

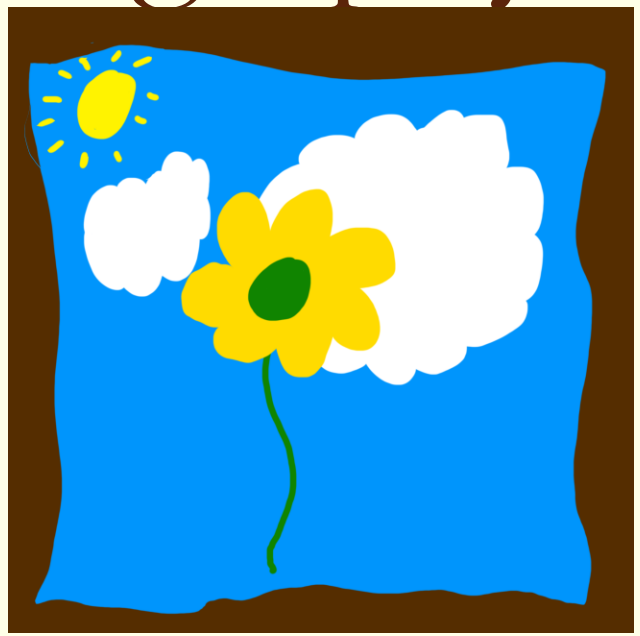
Add backdoor?

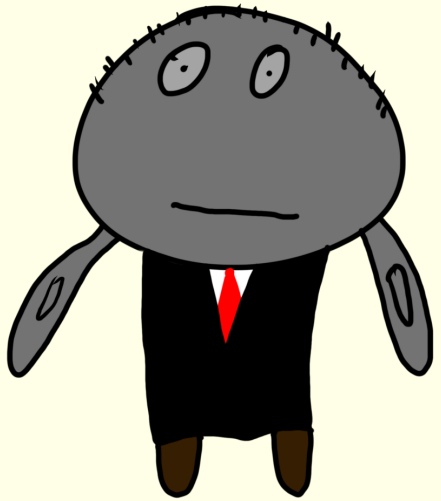
- No way, bad idea

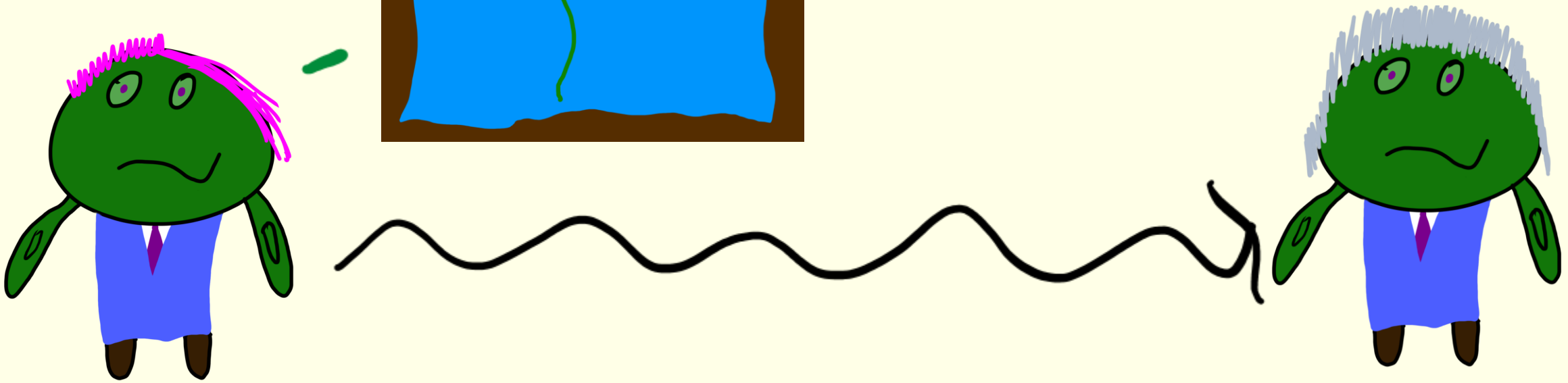
Mr. Government



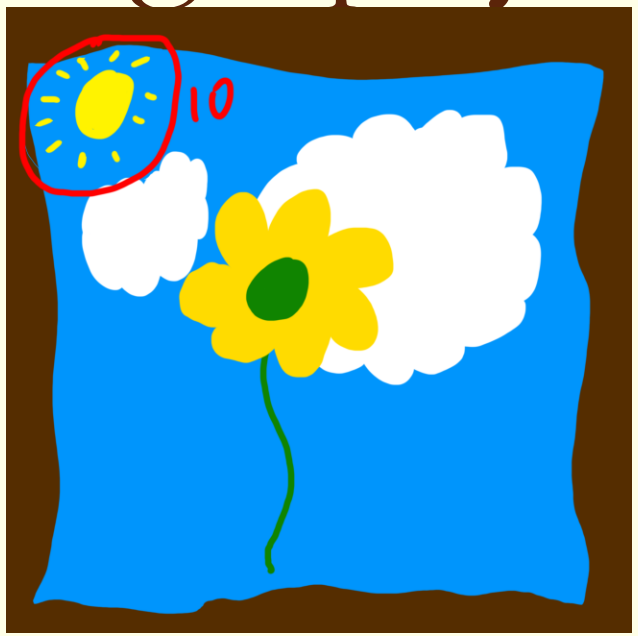
Steganography

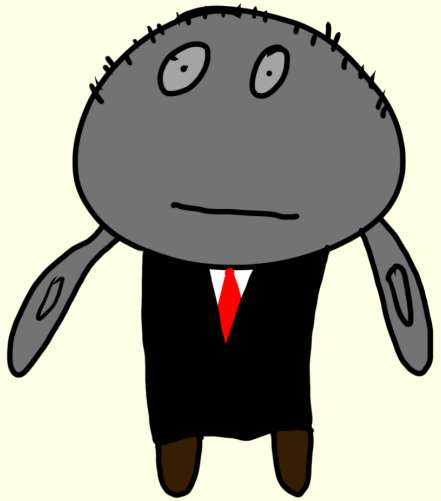




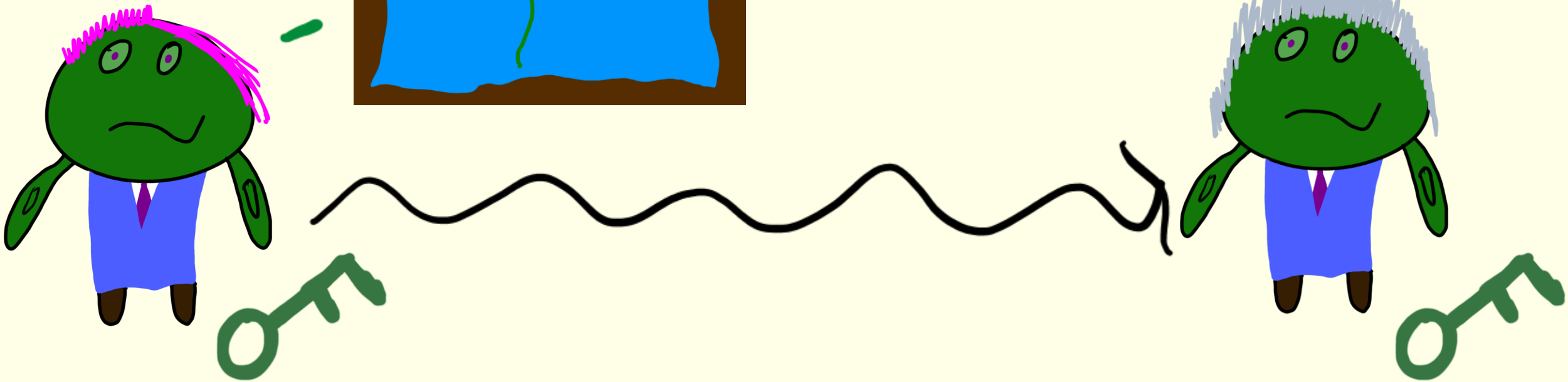


Steganography

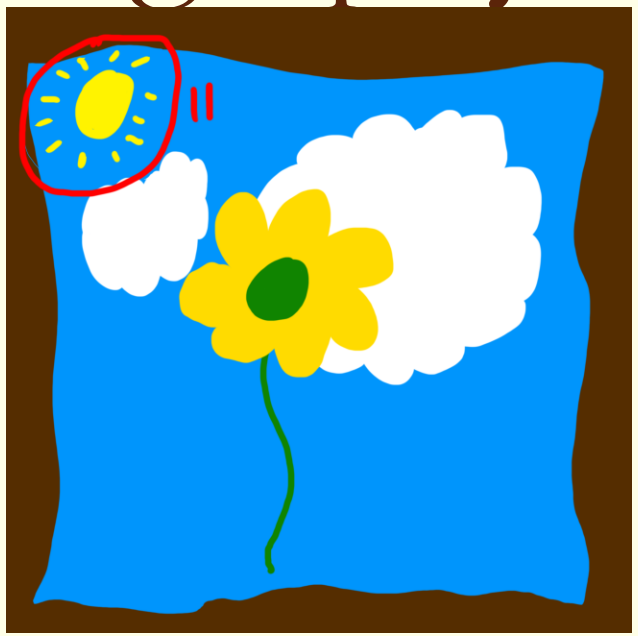


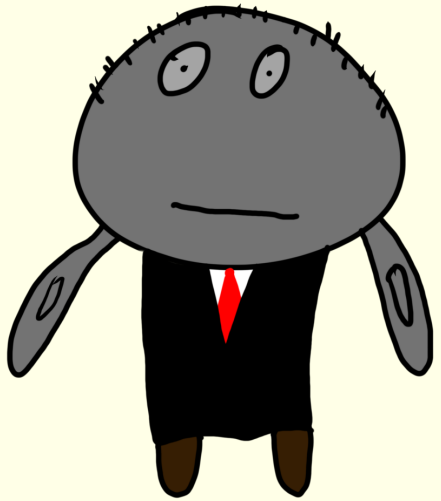


Overthrow the govt. at midnight

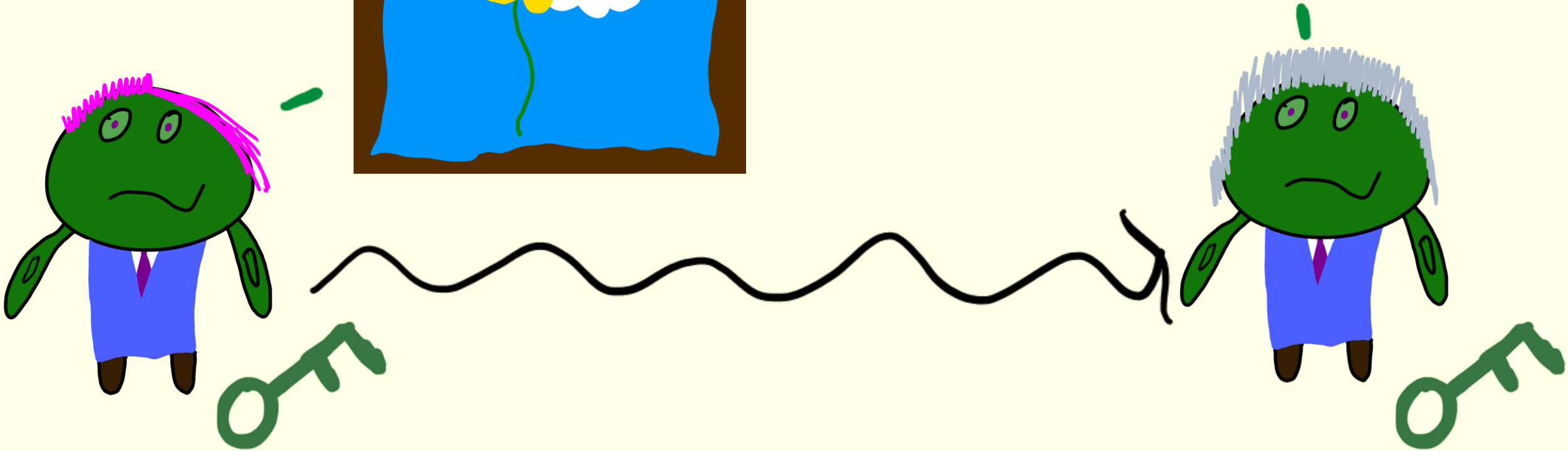


Steganography

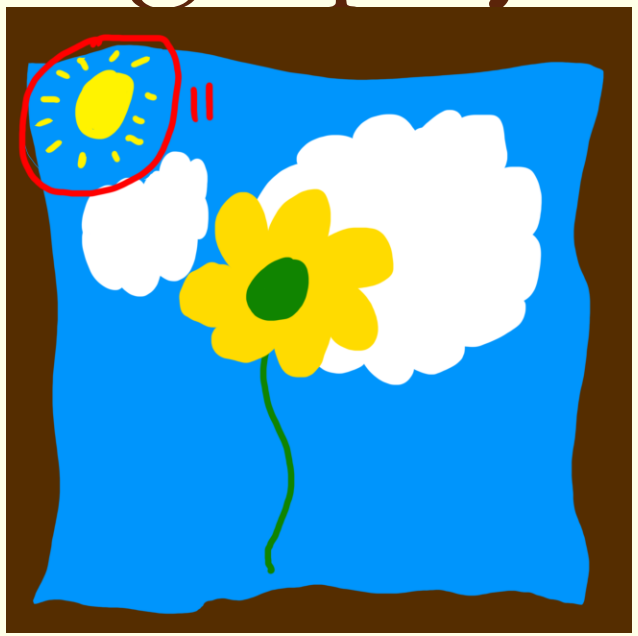


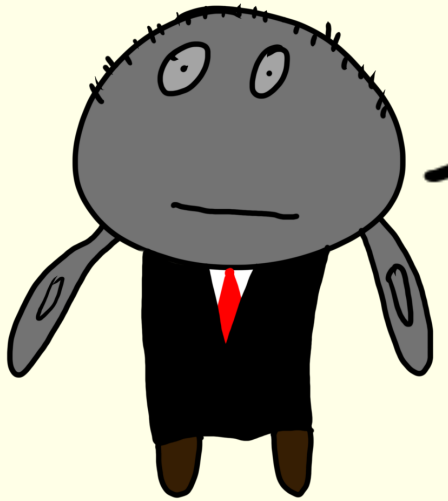


Overthrow the govt. at noon

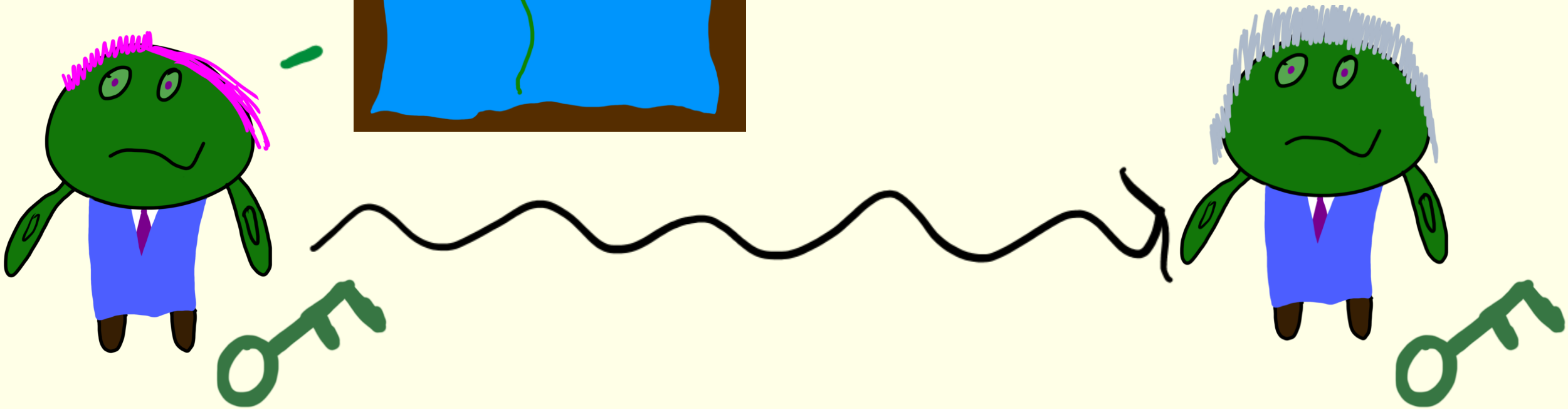


Steganography

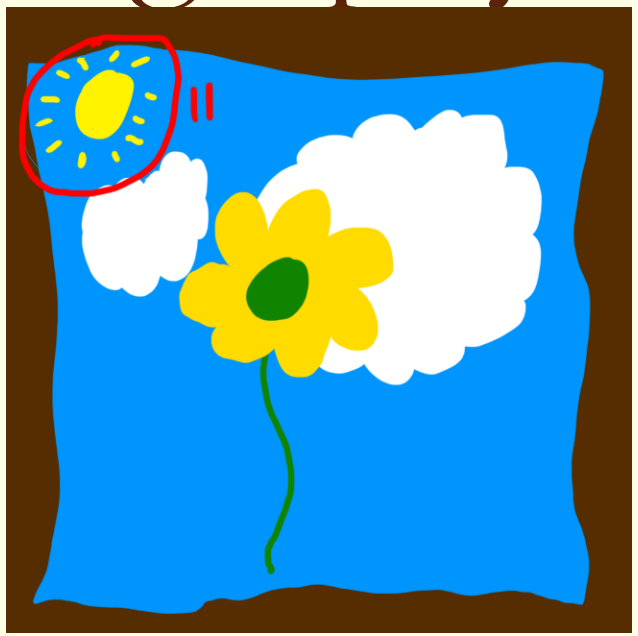


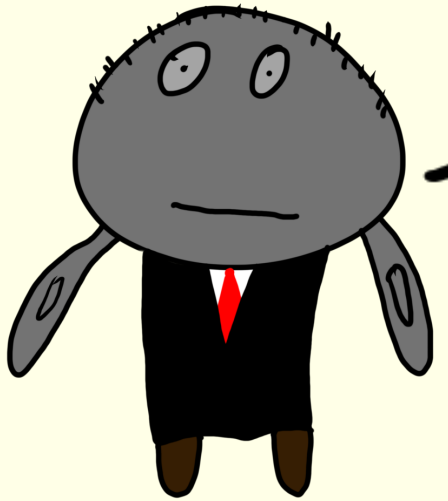


Looks like (comp. indis.) an honest photo to me.



Steganography





Looks like (comp. indis.) an honest photo to me.

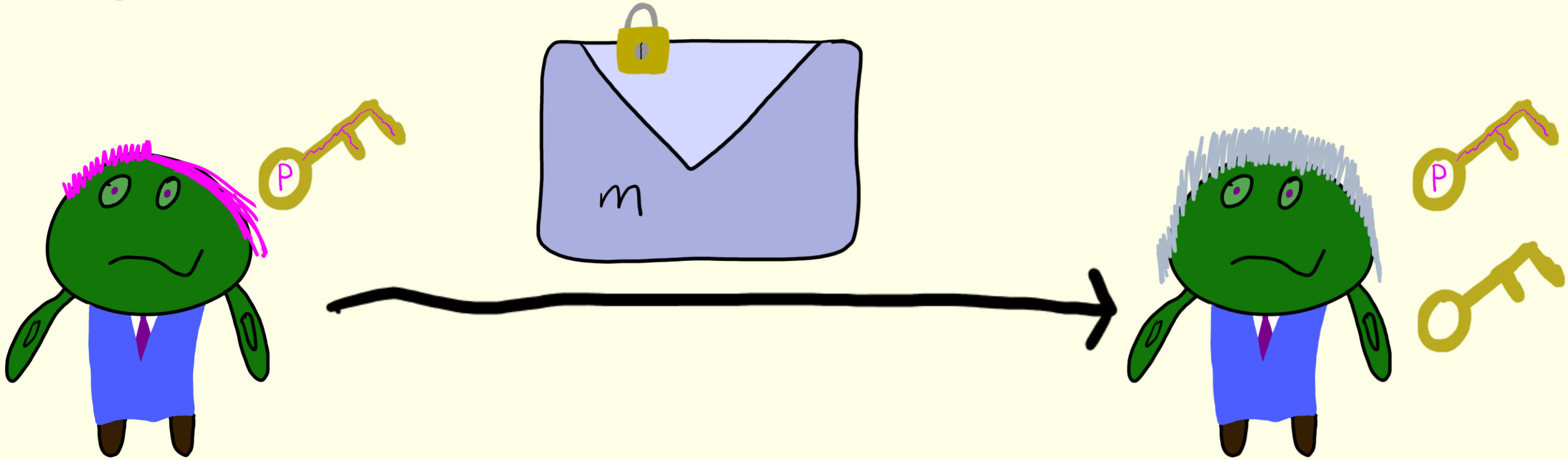
ALWAYS possible (w/ enough randomness)

Steganography

What must always be random?

Steganography

What must always be random?



Anamorphic Encryption

If you backdoor encryption, people will just use the subliminal channel.

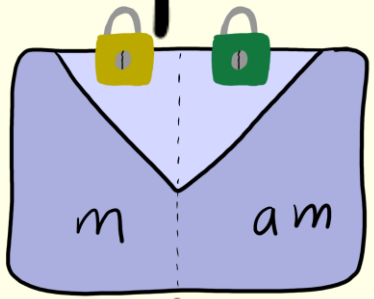
[HPRV19, PPYZ22]

Anamorphic Encryption

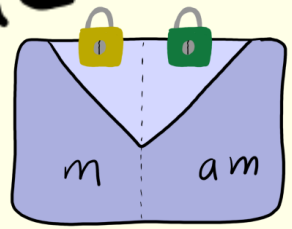
Given encryption scheme
(Gen, Enc, Dec)
Anamorphic instantiation is protocol
(AGen, AEnc, ADec) formalizing
steganographic channel

Anamorphic Encryption (Gen, Enc, Dec)

$A(Gen) \rightarrow$ 

$AEnc(m, am) \rightarrow$ 

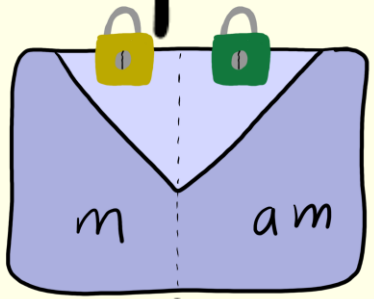
act

$ADec($  , 

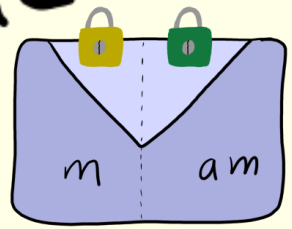
dk, act $) \rightarrow am$

Anamorphic Encryption $(Gen, \widetilde{Enc}, \widetilde{Dec})$

$A(Gen) \rightarrow$ 

$AEnc(m, am) \rightarrow$ 

act

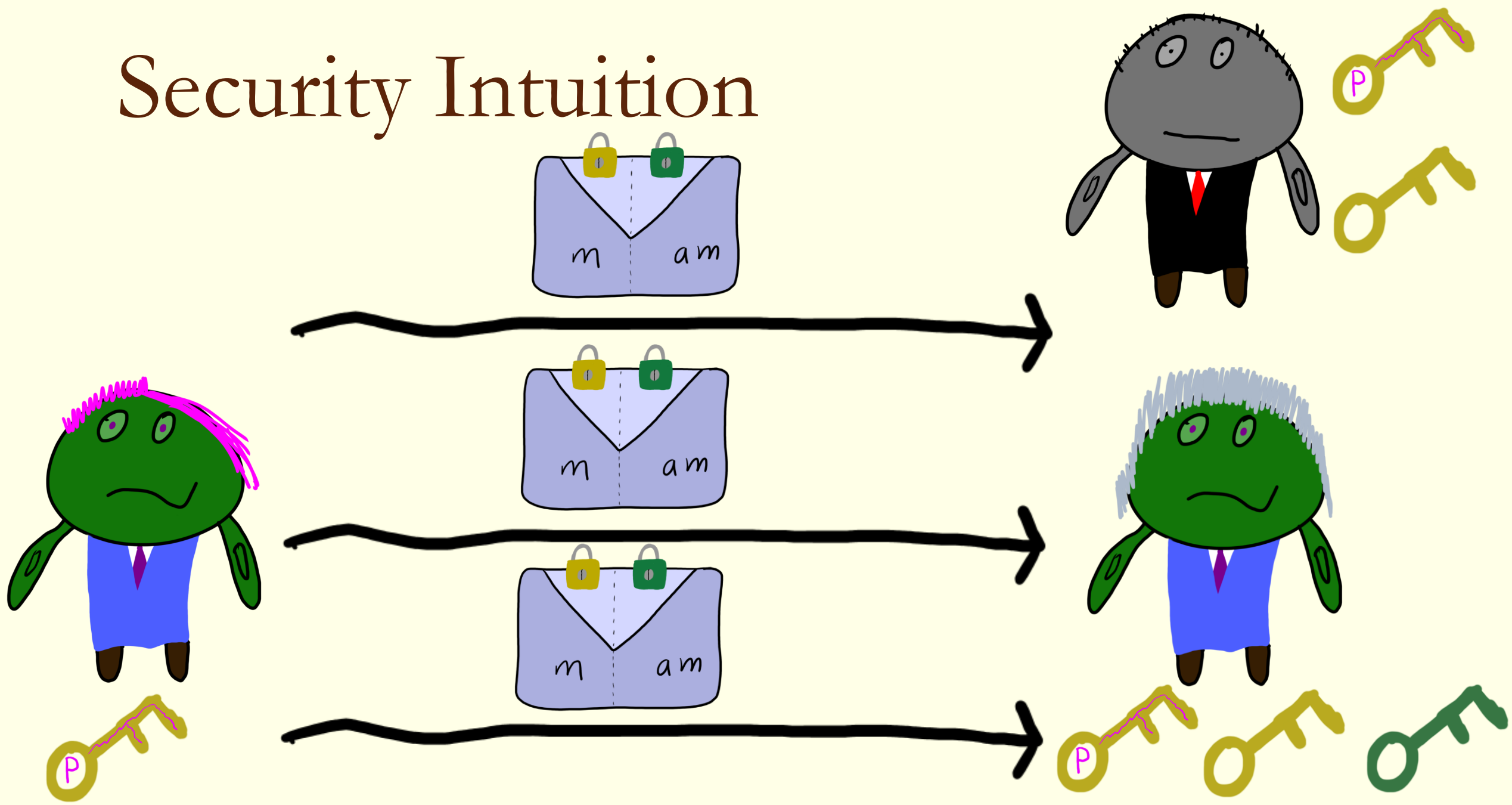
$ADec($  $,$ 

$) \rightarrow am$

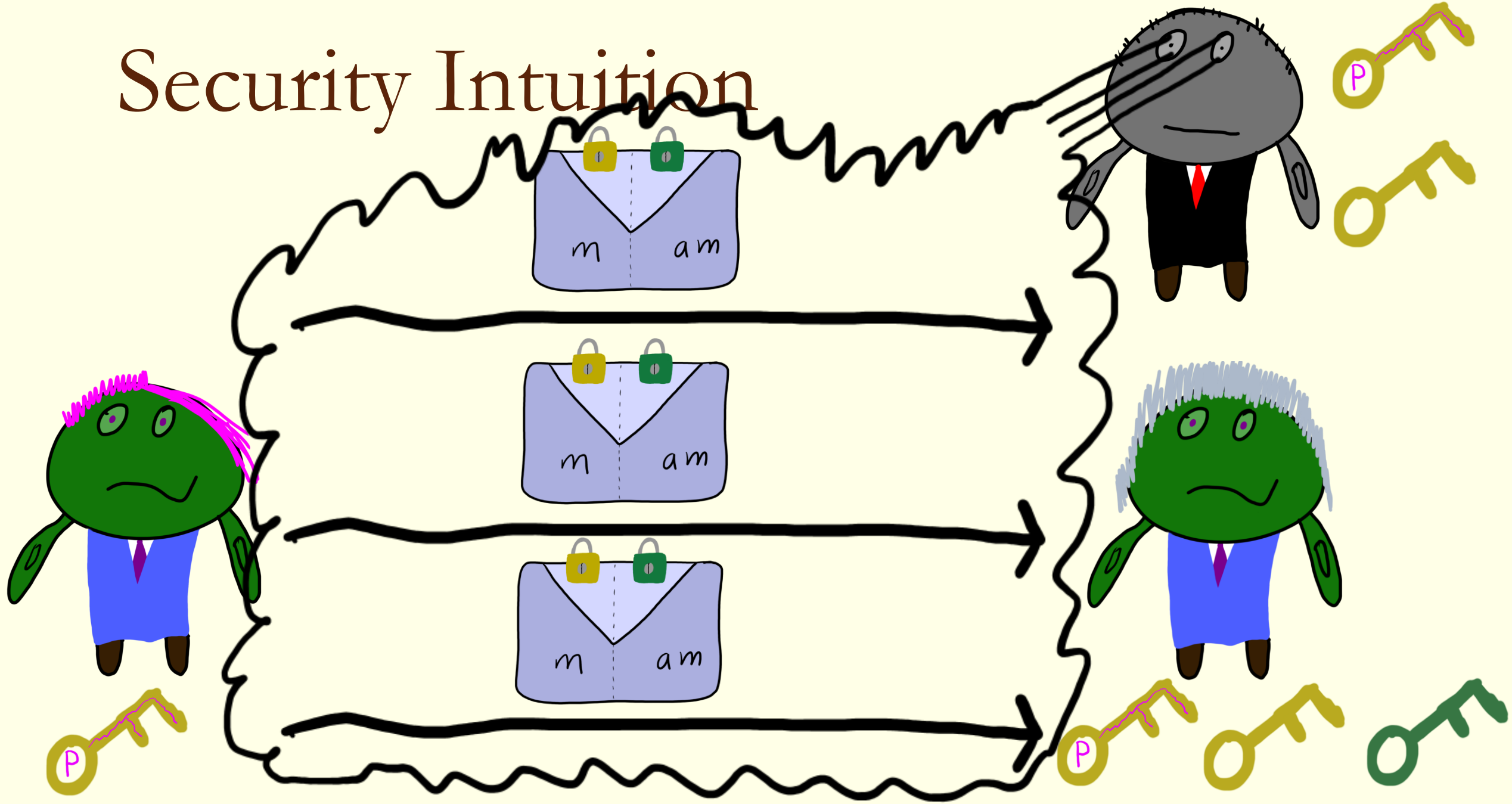
dk, act

"anamorphic instantiation of (Gen, Enc, Dec)"

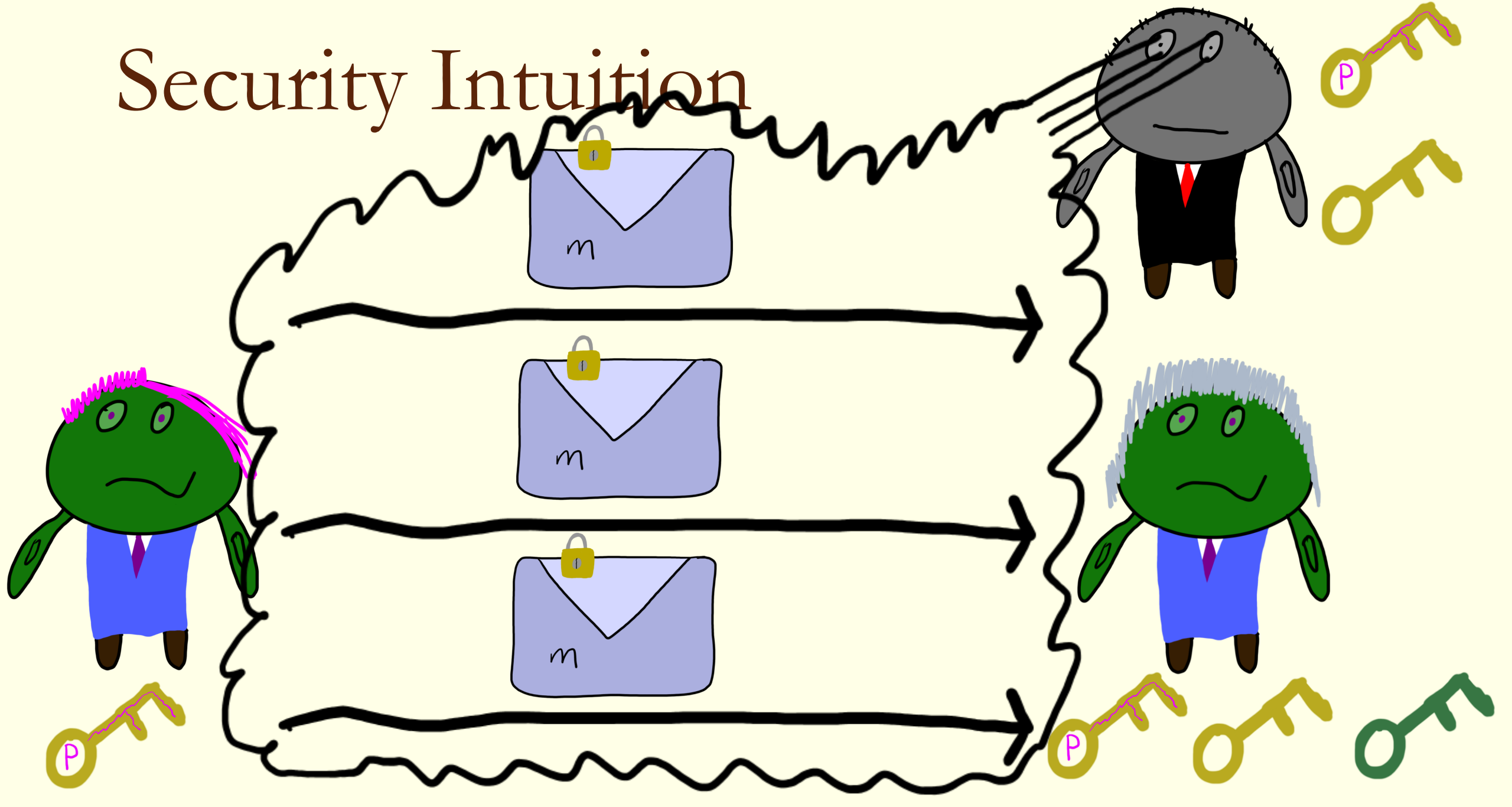
Security Intuition



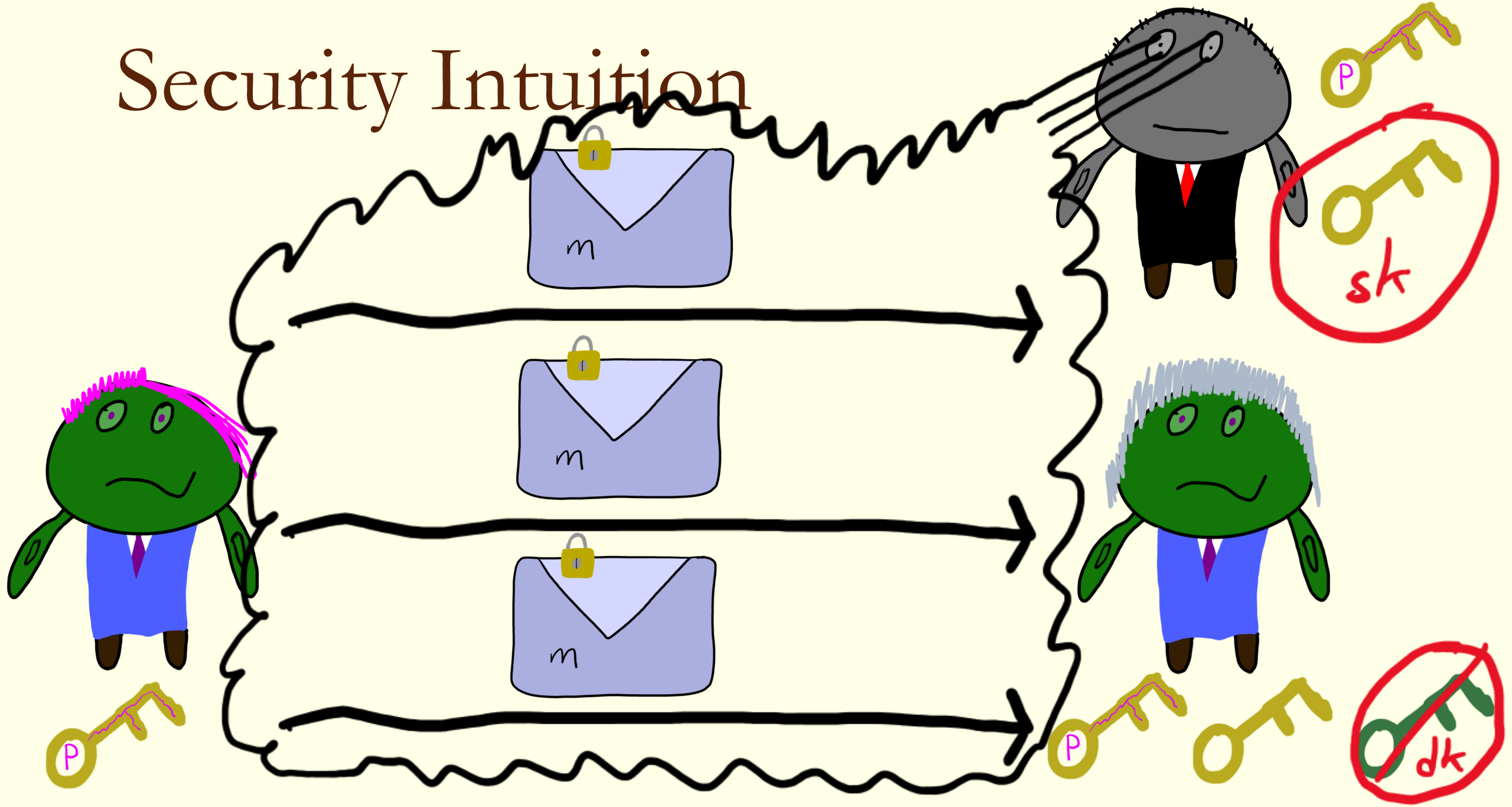
Security Intuition



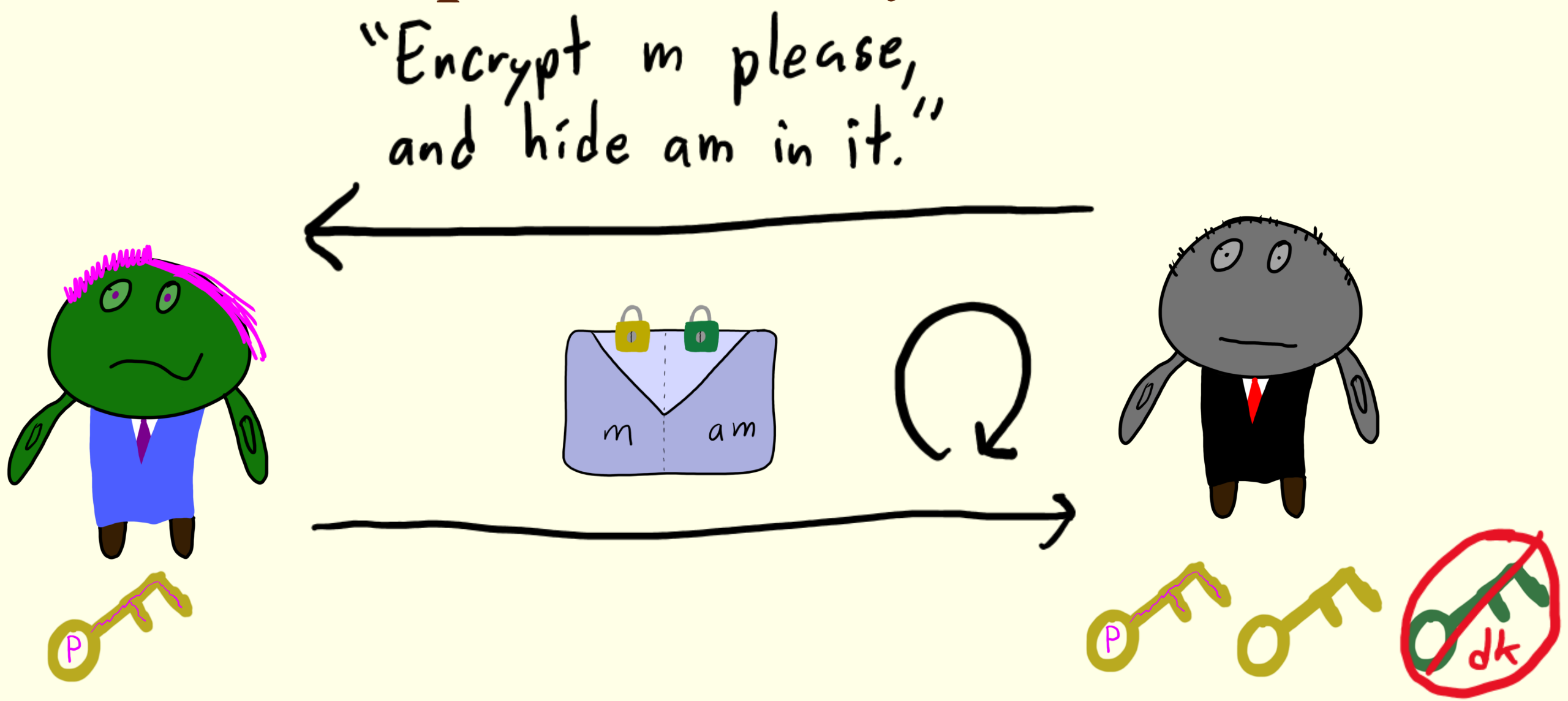
Security Intuition



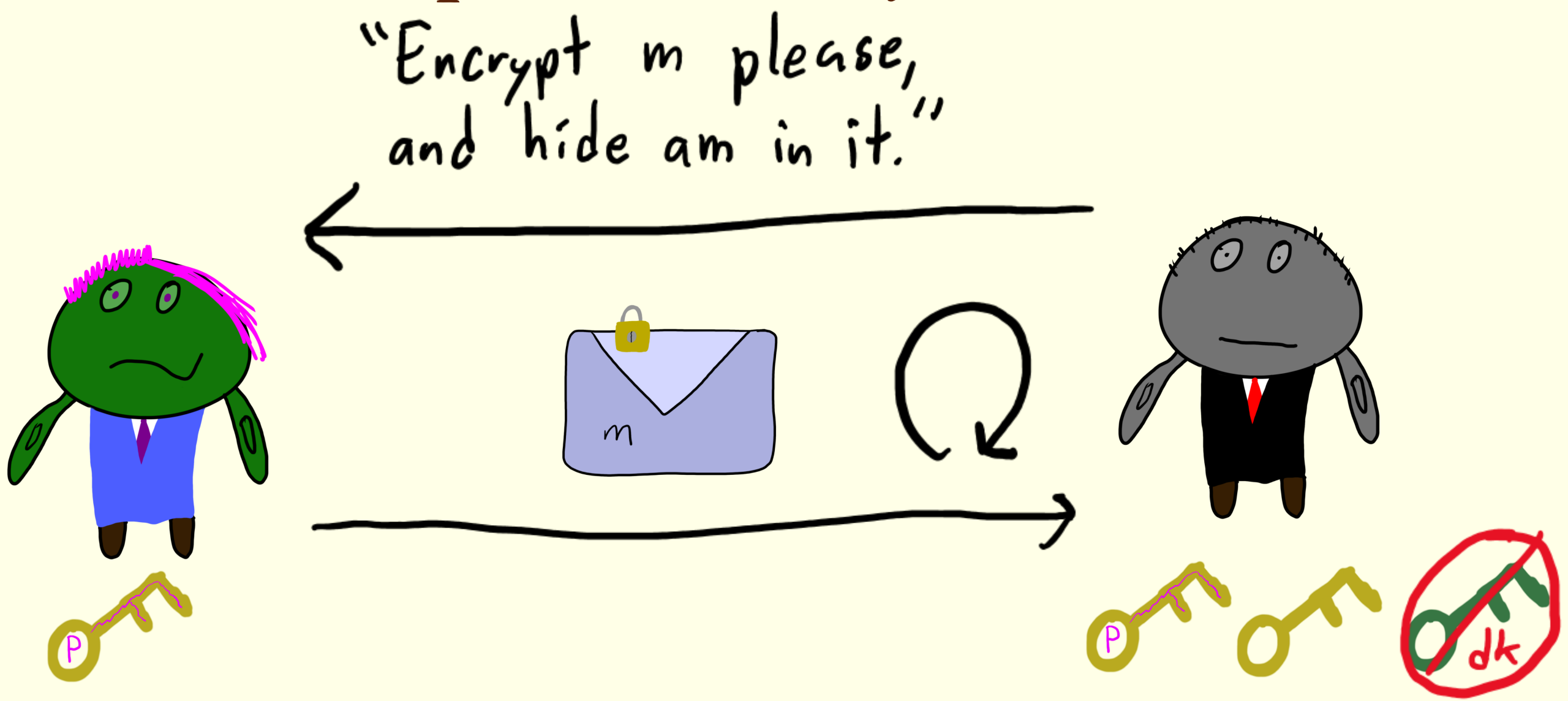
Security Intuition



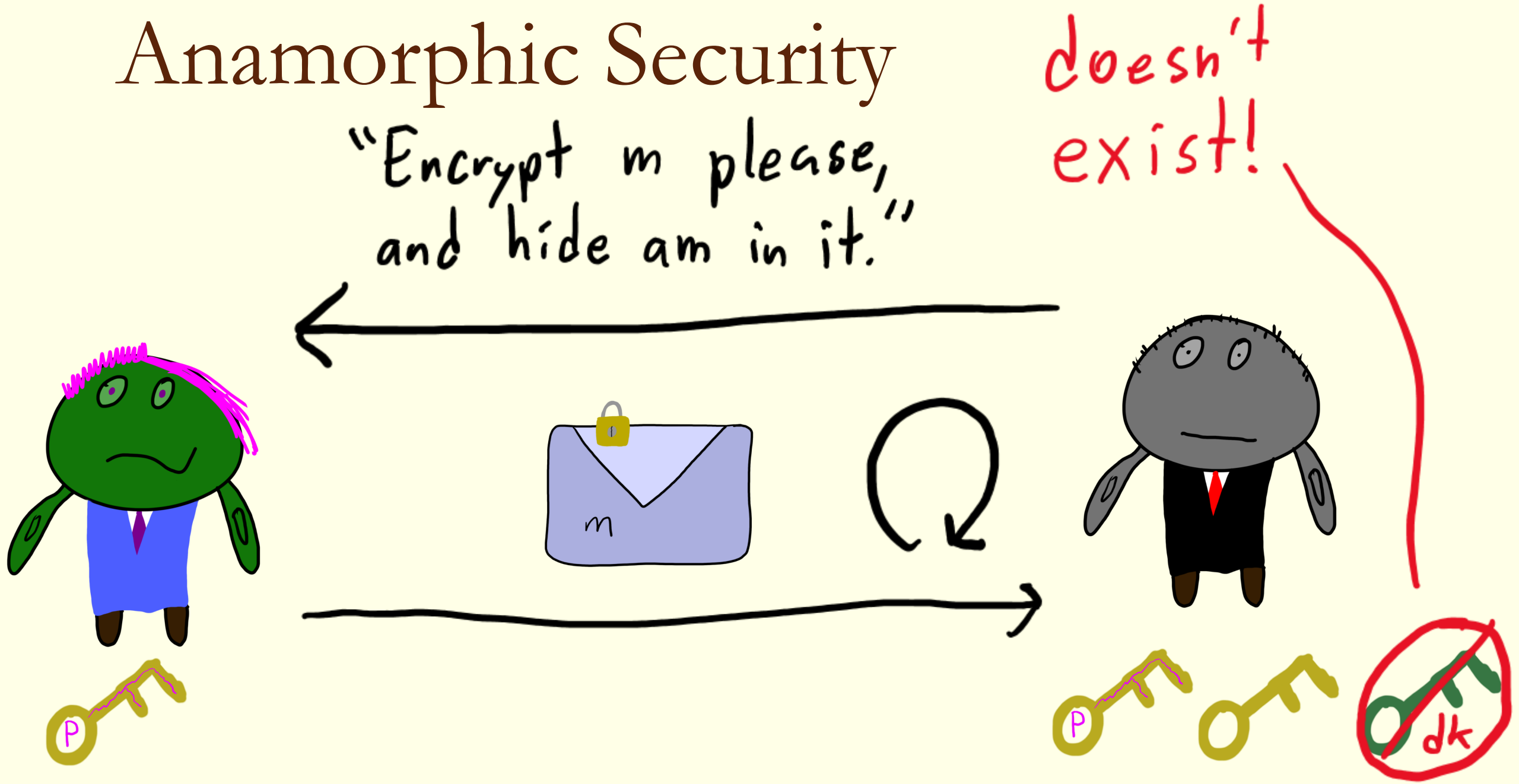
Anamorphic Security



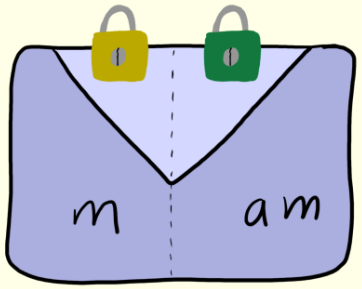
Anamorphic Security



Anamorphic Security

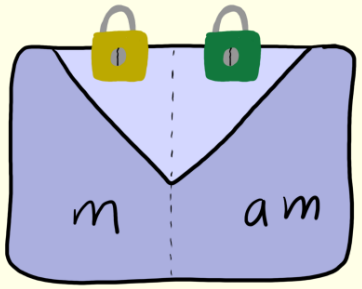


Anamorphic Encryption

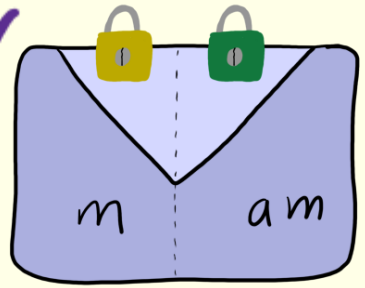


always possible by rejection sampling

Anamorphic Encryption

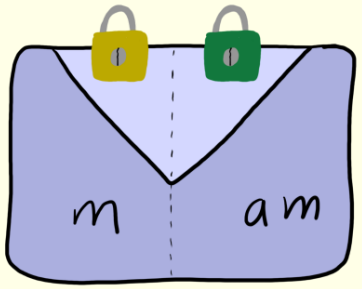


always possible by rejection sampling

$H_{\text{🔑}}$(

) = am

Anamorphic Encryption



always possible by rejection sampling

Bandwidth: $O(\log \lambda)$

Anamorphic Encryption

Generic	Linear Bandwidth
$O(\log \lambda)$ bandwidth [PPY22]	

Anamorphic Encryption

Generic

$O(\log \lambda)$ bandwidth [PPY22]

Linear Bandwidth

Paper	Applicable Schemes	Properties
[PPY22]	Naor-Yung	

Anamorphic Encryption

Generic	Linear Bandwidth		
	Paper	Applicable Schemes	Properties
$O(\log \lambda)$ bandwidth [PPY22]	[PPY22]	Naor-Yung	robust
	[BGH+24]	randomness recoverable	

Anamorphic Encryption

Generic

$O(\log \lambda)$ bandwidth

[PPY22]

Linear Bandwidth

Paper	Applicable Schemes	Properties
[PPY22]	Naor-Yung	
[BGH+24]	randomness recoverable	robust
[PPY24]	many CCA PKEs	public-key anamorphism
⋮		

Anamorphic Encryption

Generic

$O(\log \lambda)$ bandwidth

[PPY22]

Linear Bandwidth

Applicable Schemes

Paper	Applicable Schemes	Properties
[PPY22]	Naor-Yung	
[BGH+24]	randomness recoverable	robust
[PPY24]	many CCA PKEs	public-key anamorphism
⋮	([KPP+23]×2, [CGM24], ...)	

Anamorphic Encryption

Hypothesis: linear bandwidth anamorphic instantiations are always possible.

Anamorphic Encryption

Hypothesis: linear bandwidth anamorphic instantiations are always possible.

Spoiler: NO

Philosophy

Philosophical Question

Who picks what PKE schemes are legal?

Dictatoria

Wants to read all messages (universal backdoor)

Dictatoria

Wants to read all messages (universal backdoor)

Privacy against foreign nations

Dictatoria

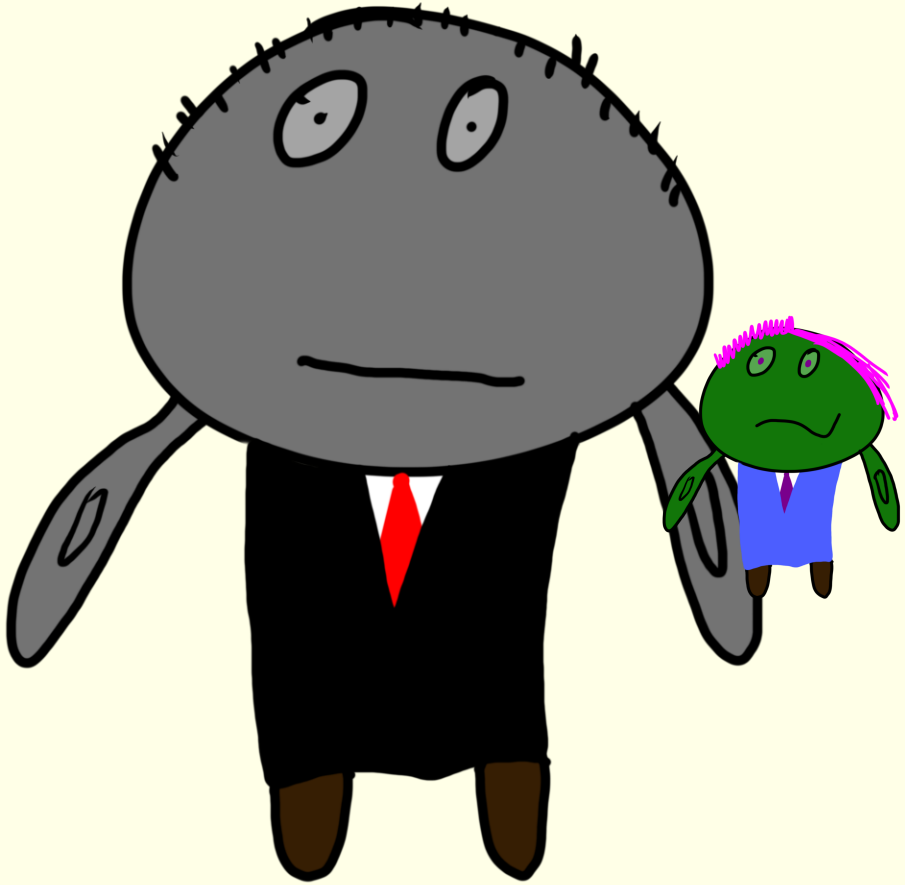
Wants to read all messages (universal backdoor)

Privacy against foreign nations

Outlaw non-trivial anamorphism

Warrantland

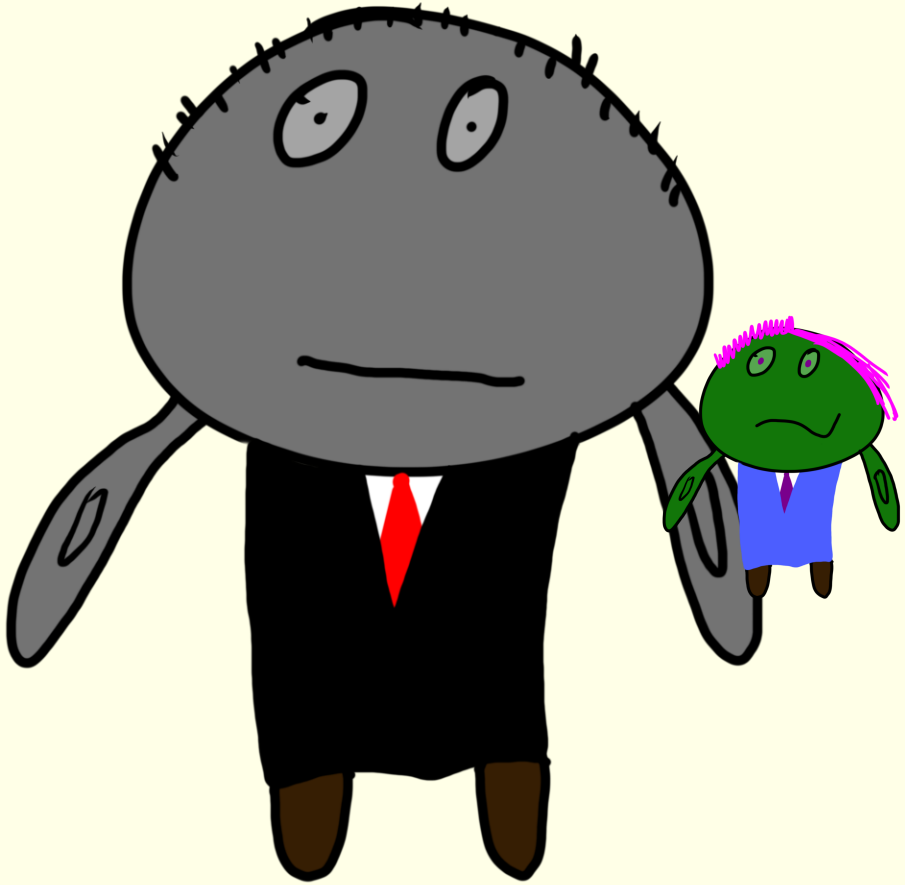
Wants to read messages when warrant issued



Warrantland

Wants to read messages when warrant issued

Privacy against itself with no warrant

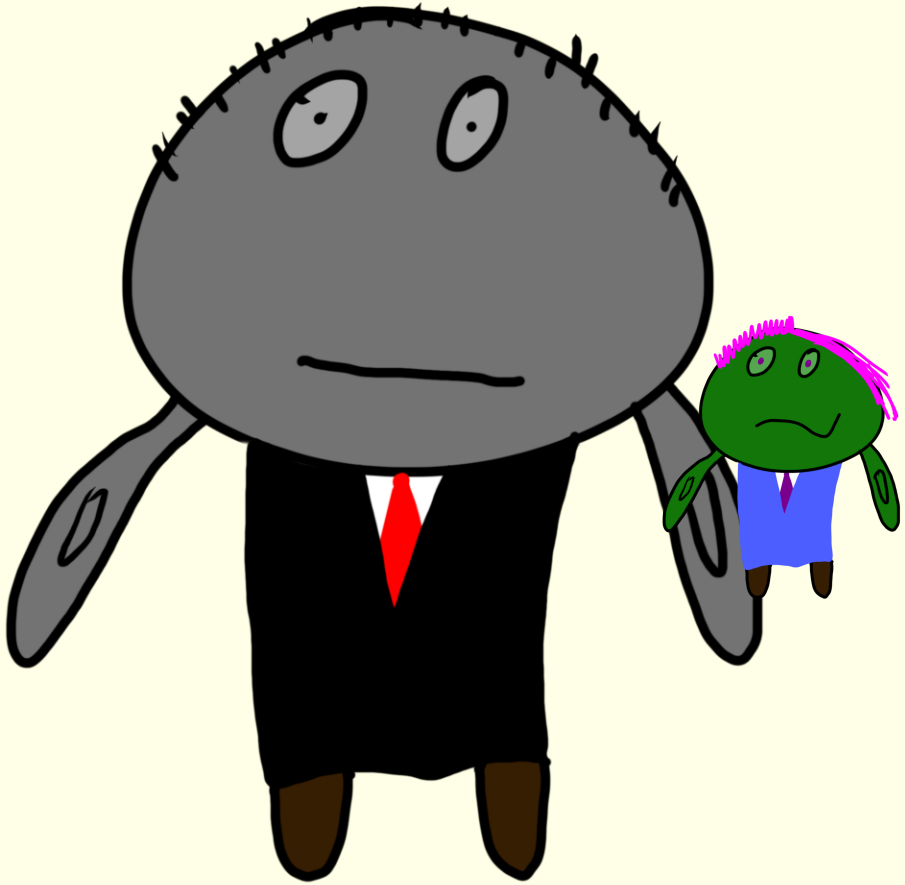


Warrantland

Wants to read messages when warrant issued

Privacy against itself with no warrant

Outlaw non-trivial anamorphism



Privatopia

Privacy against itself now and in the future

Privatopia

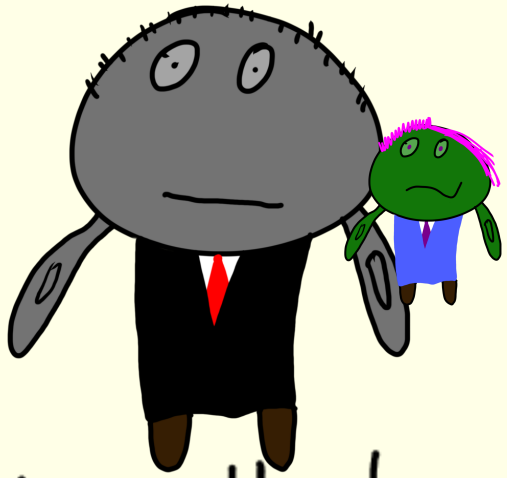
Privacy against itself now and in the future

Wants to standardize anamorphic encryption

Main Philosophical Question

Are there schemes which make

Dictatoria



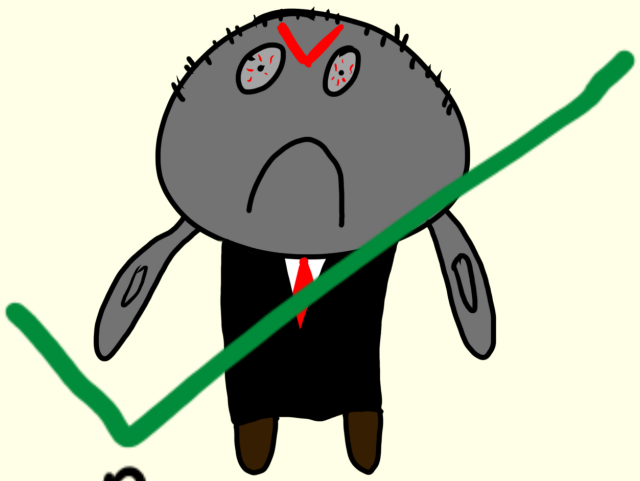
Warrantland

Privatopia

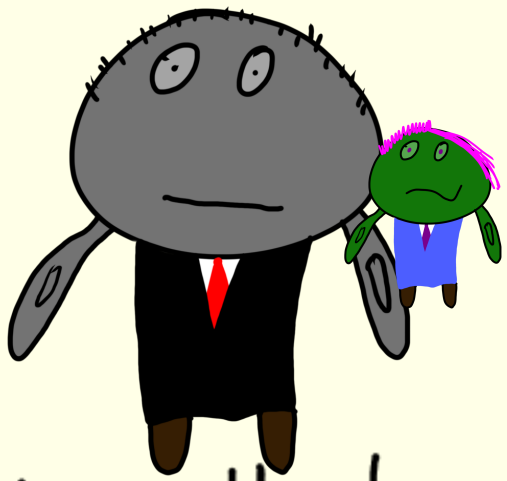
happy?

Main Philosophical Question

Are there schemes which make



Dictatoria



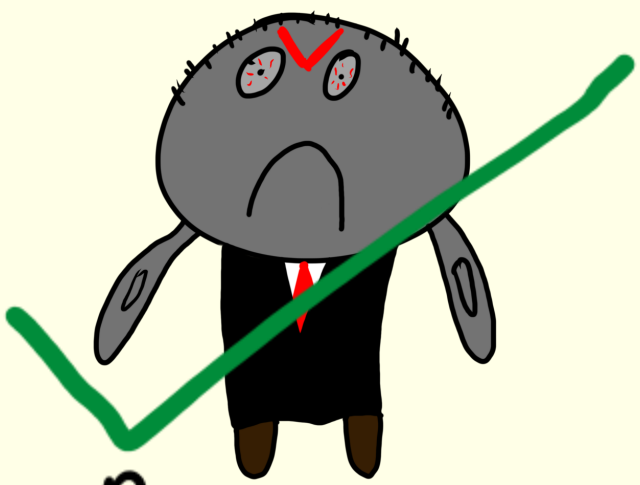
Warrantland

Privatopia

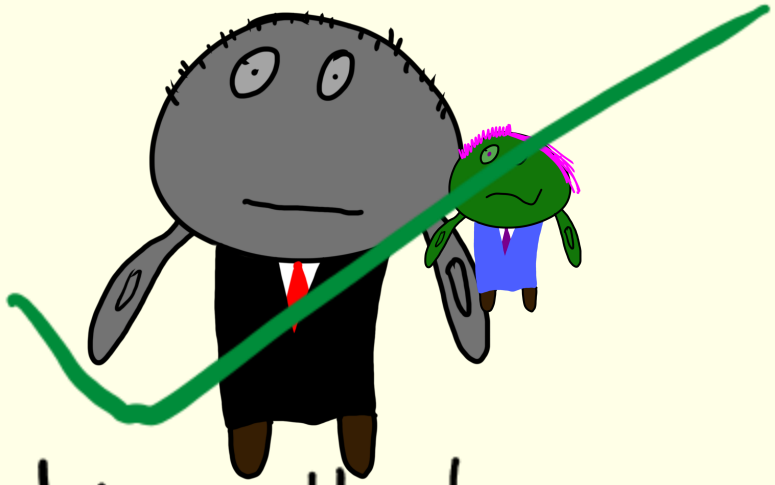
happy?

Main Philosophical Question

Are there schemes which make



Dictatoria



Warrantland

Primstopia

happy?

Results

Anamorphic Resistant Encryption

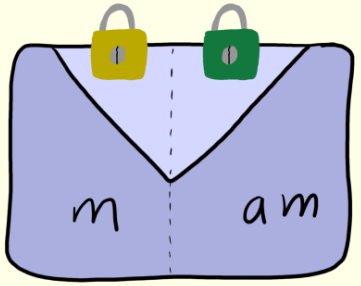
(Gen, Enc, Dec) such that no non-trivial anamorphic instantiation exists.

Anamorphic Resistant Encryption

(Gen, Enc, Dec) such that no non-trivial anamorphic instantiation exists.

ALL (AGen, AEnc, ADec)

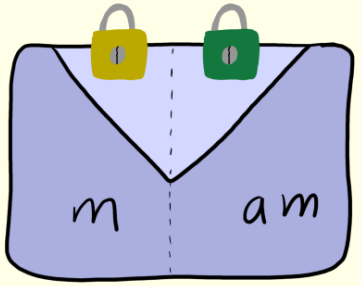
have $|am| = O(\log \lambda)$



Anamorphic Resistant Encryption

(Gen, Enc, Dec) such that no non-trivial anamorphic instantiation exists.

ALL (AGen, AEnc, ADec)



have $|am| = O(\log \lambda)$

ARE

Dictatoria

Dictatoria

ARE w/ universal backdoor.

Dictatoria

ARE w/

universal backdoor.

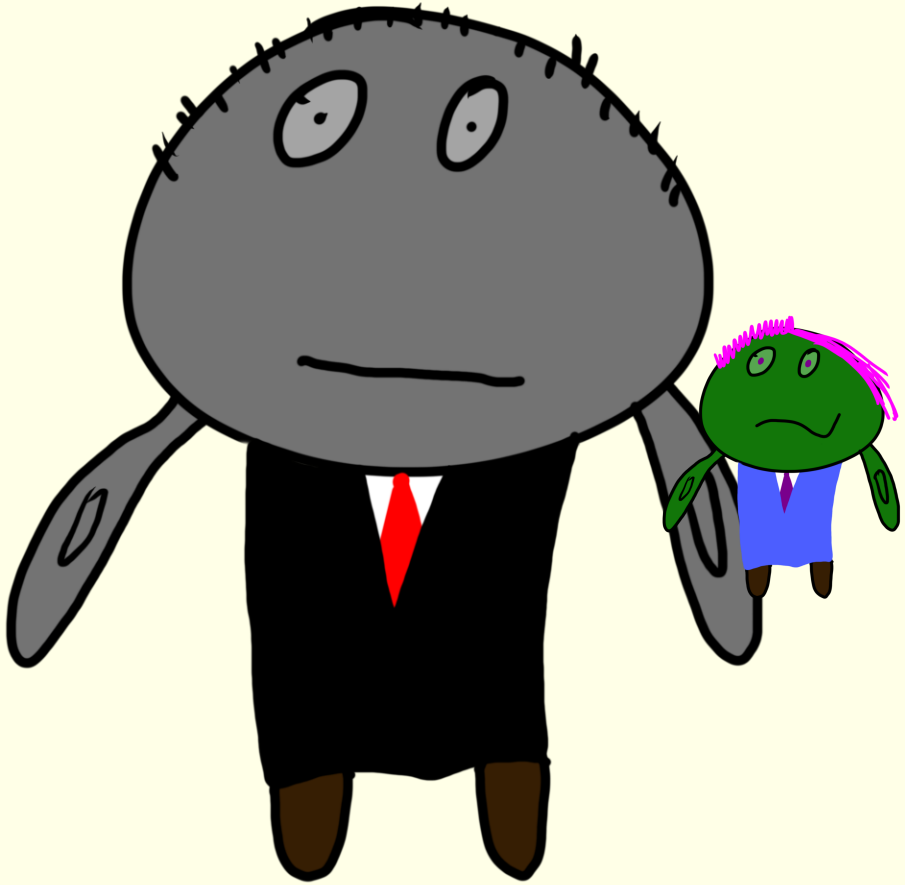
Dictator can read all messages & detect anamorphism without secret-key access

Dictatoria ~~ARE~~ in ROM

universal backdoor.

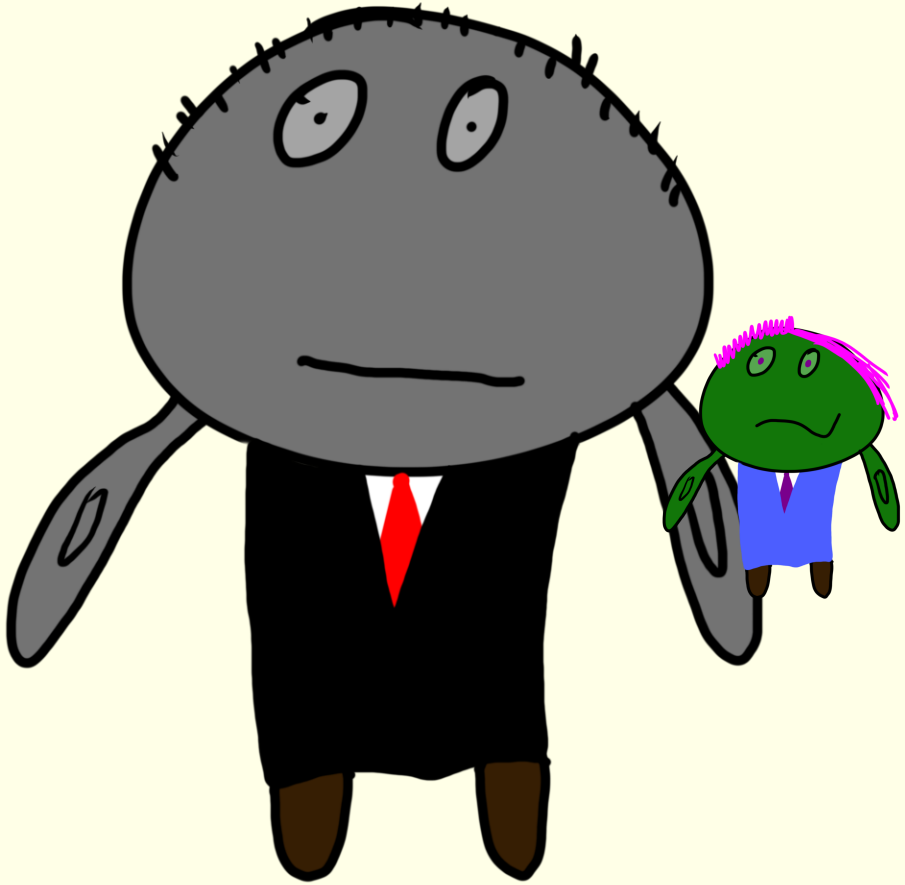
Dictator can read all messages & detect anamorphism <u>without</u> secret-key access

Warrantland



Warrantland

ARE which needs secret key access.



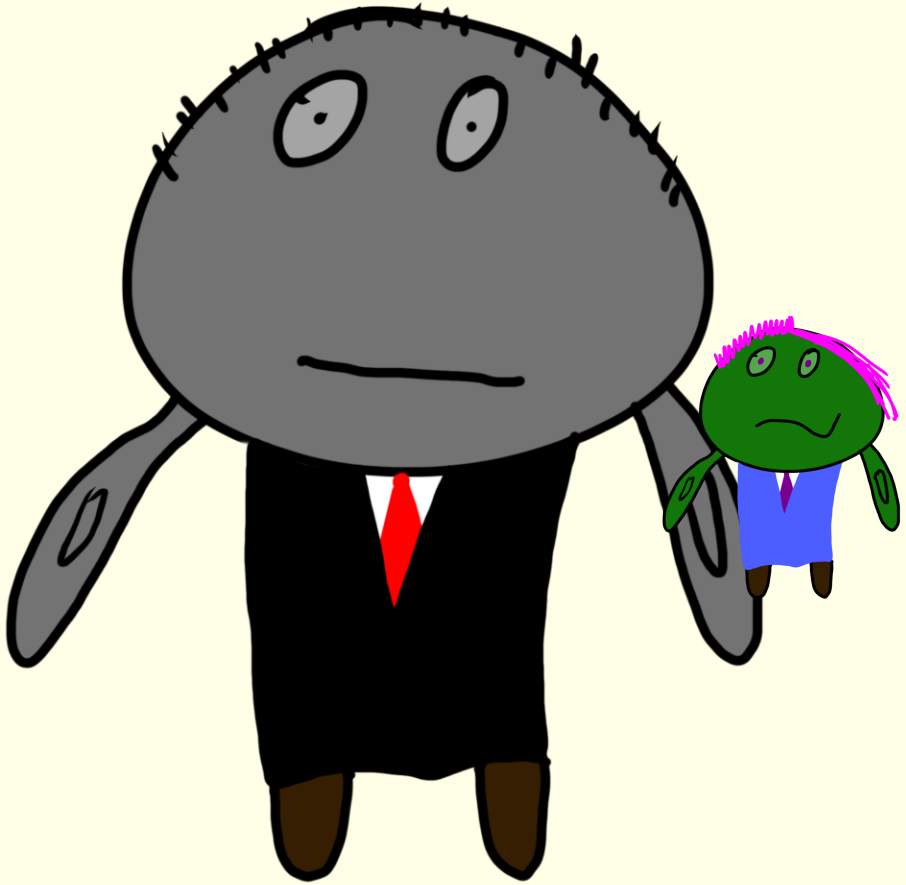
Warrantland

ARE which needs secret key access.

If  hidden, secure against govt. w/ 

sk

backdoor

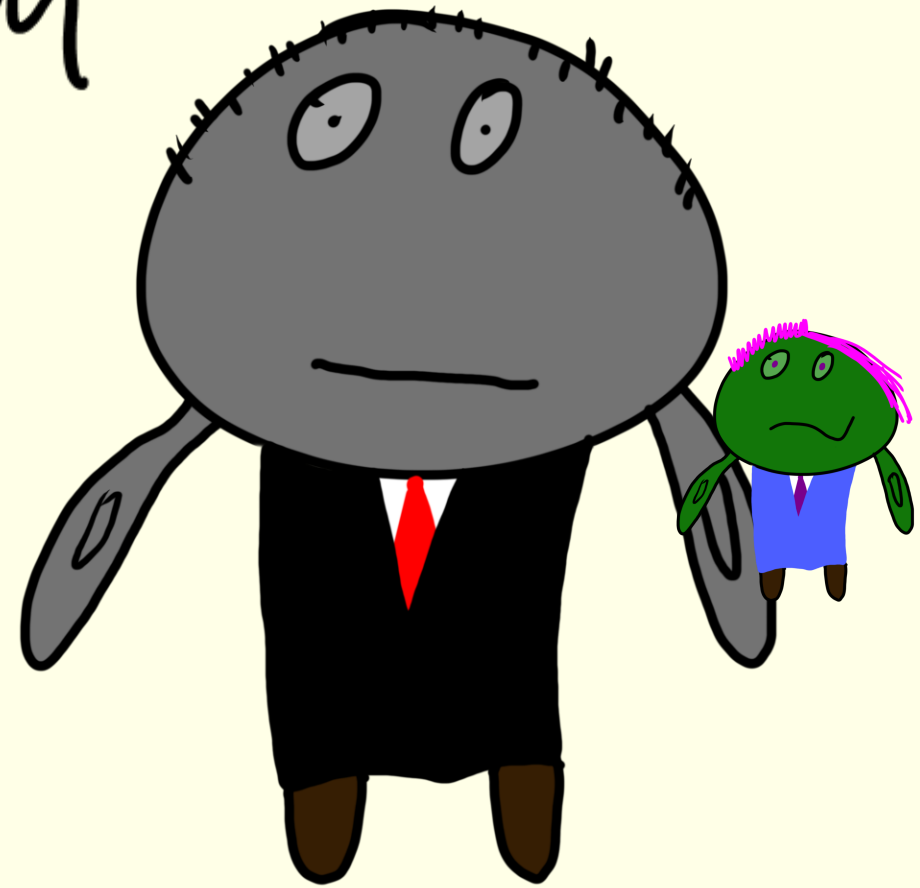


Warrantland in ROM

ARE which needs secret key access.

If  hidden, secure against govt. w/ 

backdoor

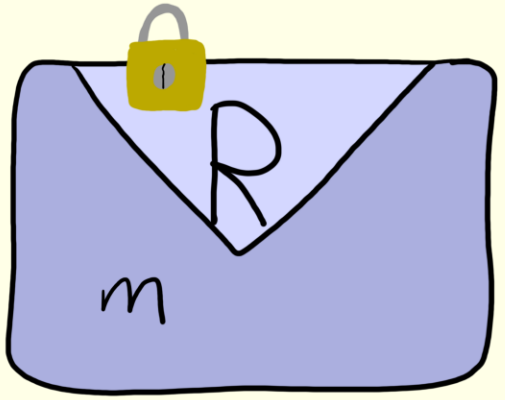


ARE

Construction

Anamorphic Resistant Encryption

Key plan: "only way to bias

$Enc(pk, m; R) \rightarrow$ 

is to do rejection sampling"

Anamorphic Resistant Encryption

Idea #1: Replace R w/ RO(R)

$$Enc(pk, m; R) = E(pk, m; RO(R))$$

Anamorphic Resistant Encryption

Idea #1: Replace R w/ RO(R)

(Only way to bias RO(R) is rej. sampling)

$$Enc(pk, m; R) := E(pk, m; RO(R))$$

Anamorphic Resistant Encryption

If

$AEnc(m, am) =$

Anamorphic Resistant Encryption

If

$AEnc(m, am) =$ 

then $RO(R_{am})$ can only provide

$\approx \log \lambda$ bits of info on am

Anamorphic Resistant Encryption

If

$AEnc(m, am) =$

might not be the case.

then $RO(R_{am})$ can only provide

$\approx \log \lambda$ bits of info on am

Anamorphic Resistant Encryption

Key question: how to force

$AEnc(m, am) =$ 

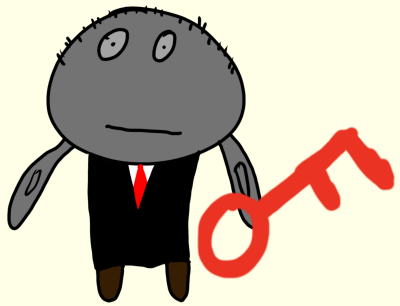
?

Anamorphic Resistant Encryption

Key question: how to force

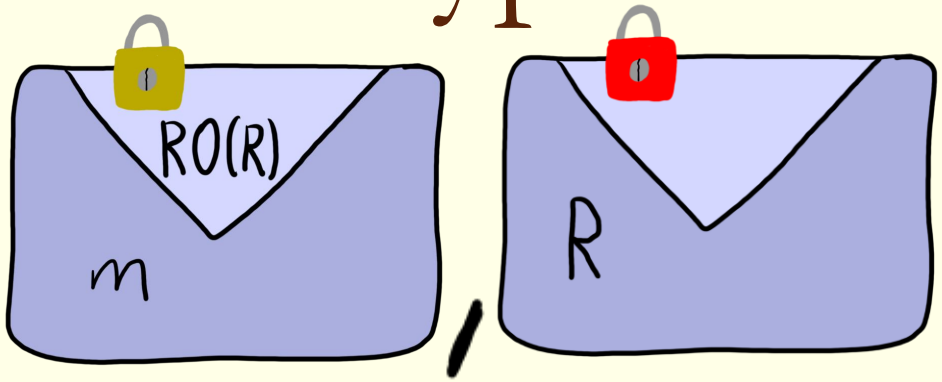
$AEnc(m, am) =$ 

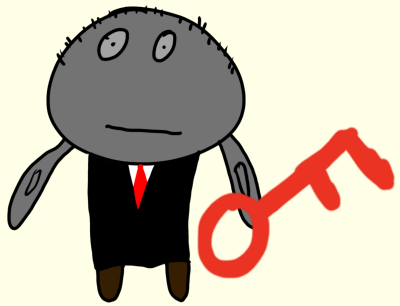
?

Idea 2: tell  R

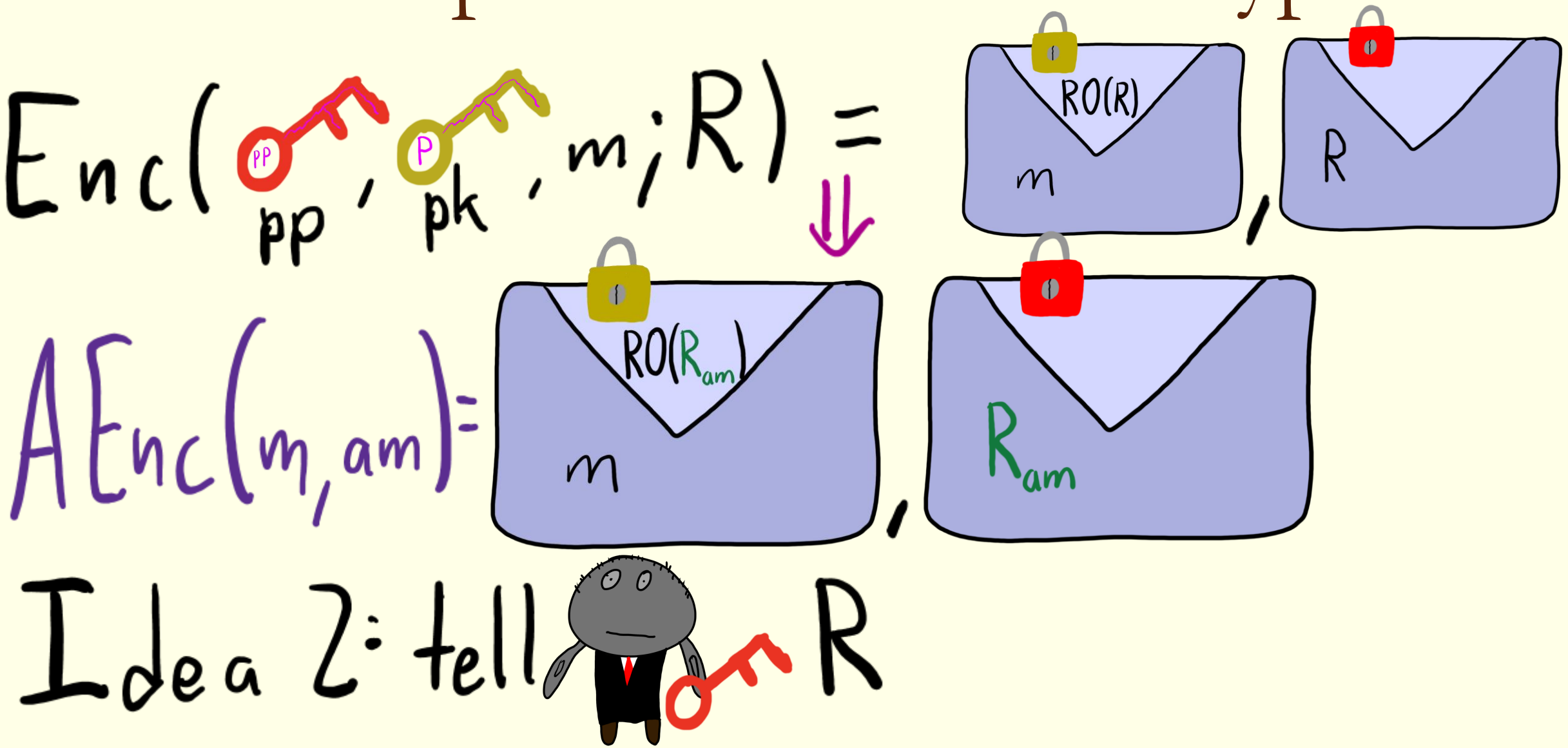
Anamorphic Resistant Encryption

$Enc(pp, pk, m; R) =$

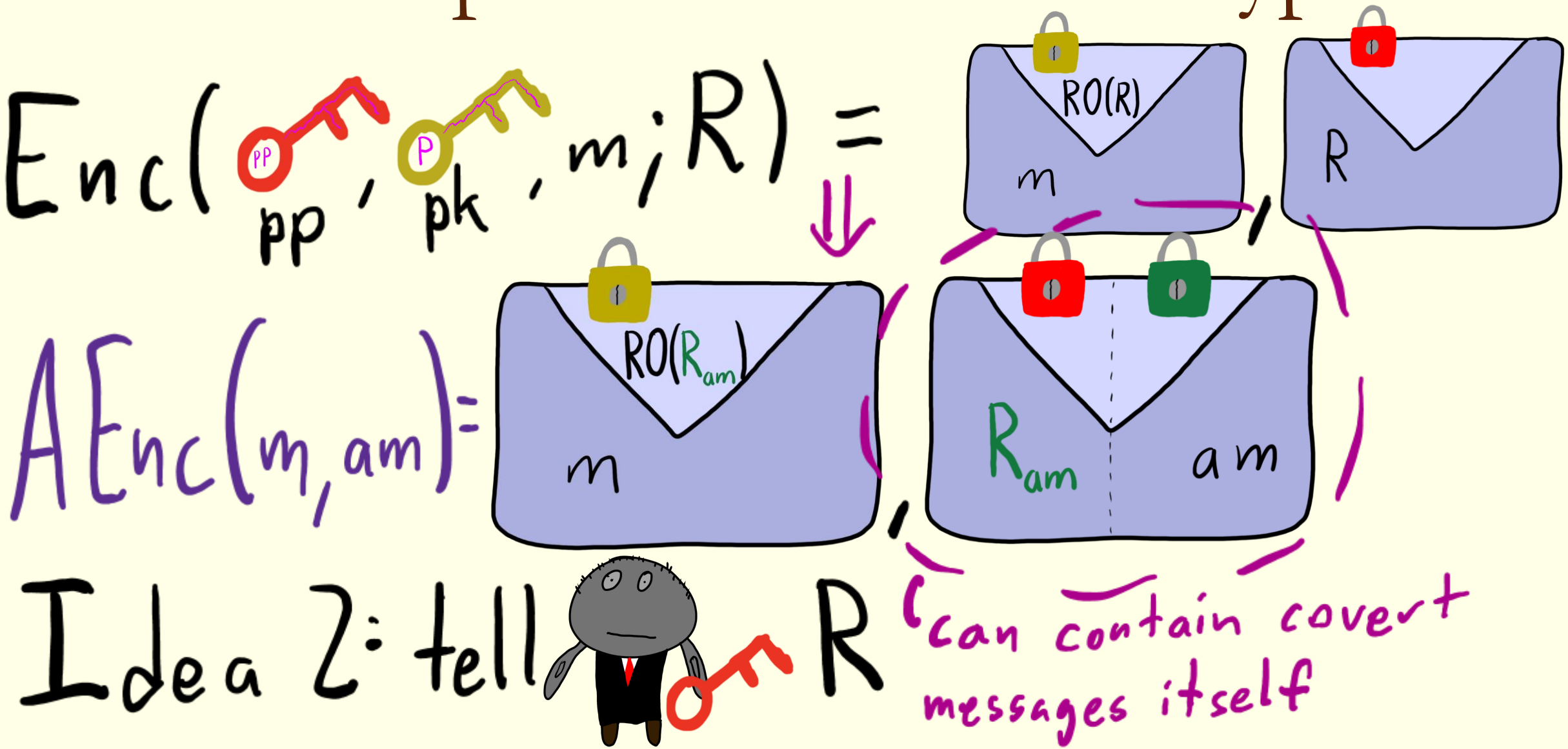


Idea 2: tell  R

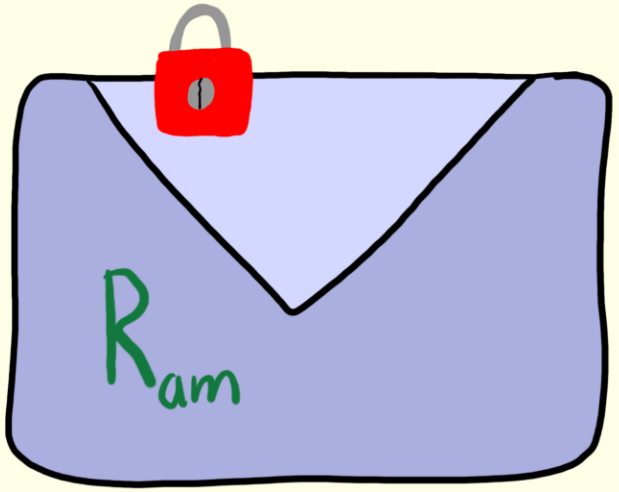
Anamorphic Resistant Encryption



Anamorphic Resistant Encryption



Deterministic Encryption

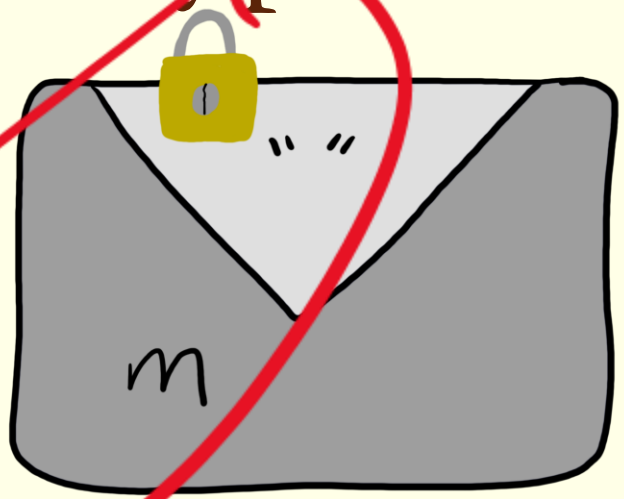
If 

is not random,

can't contain any anamorphic message.

Deterministic Encryption

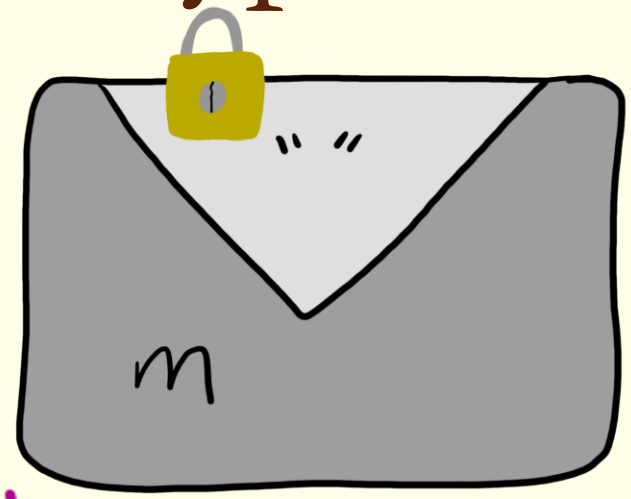
$DEnc(pk, m) :=$



usually impossible

Deterministic Encryption

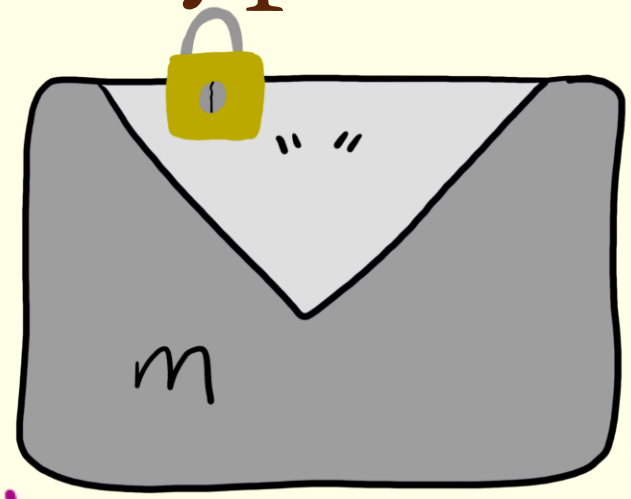
$DEnc(pk, m) =$



Possible in restricted circumstances

Deterministic Encryption

$DEnc(pk, m) =$

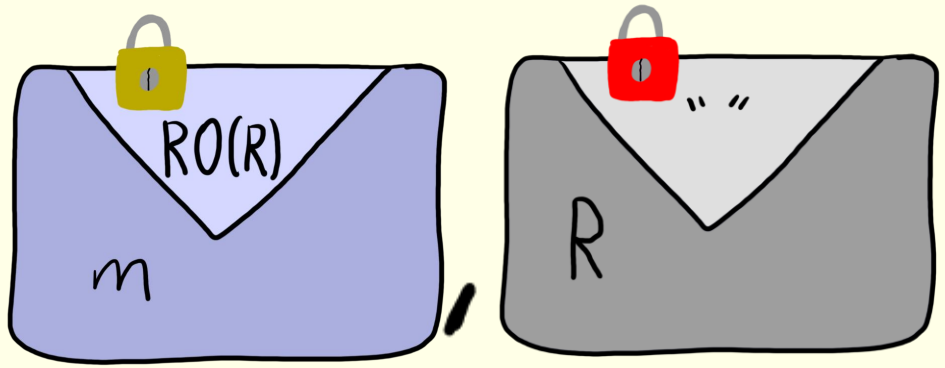


Possible in restricted circumstances

Including this one! (with work)

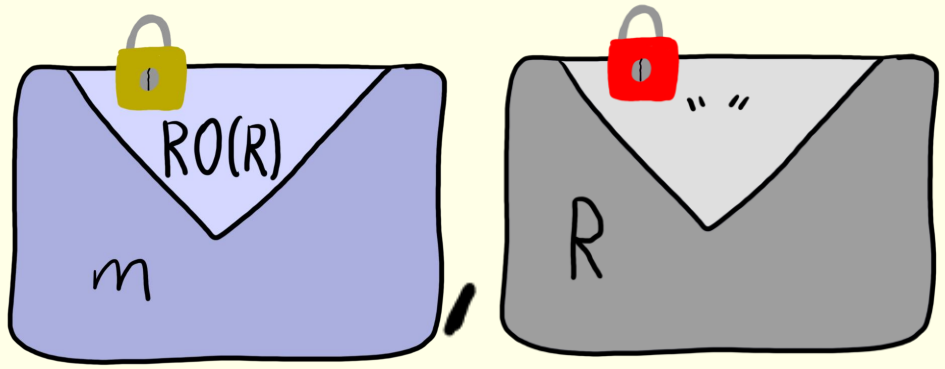
Final Construction

$Enc(pp, pk, m; R) =$



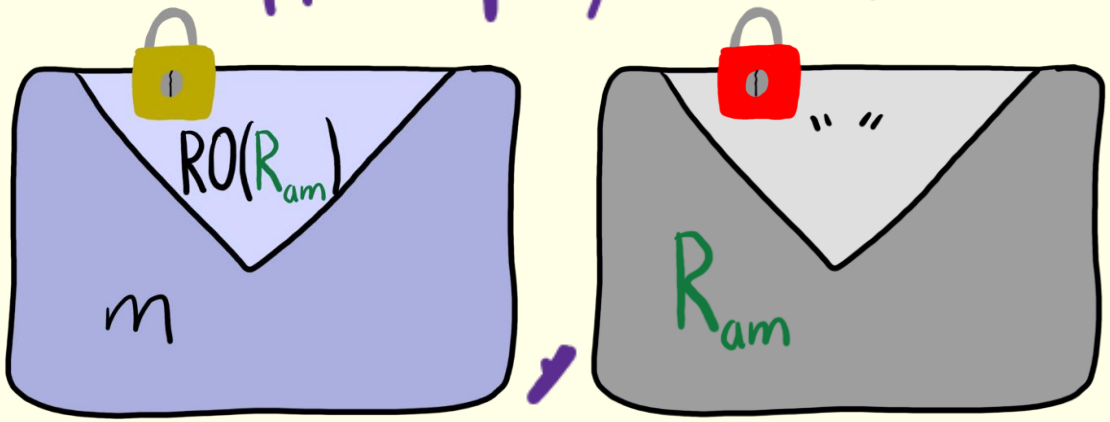
Final Construction

$Enc(pp, pk, m; R) =$



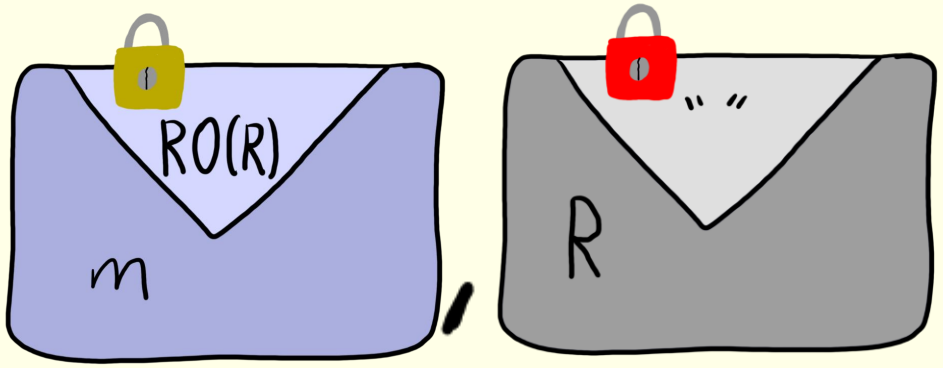
$AEnc(pp, pk, ak, m, am)$

$=$

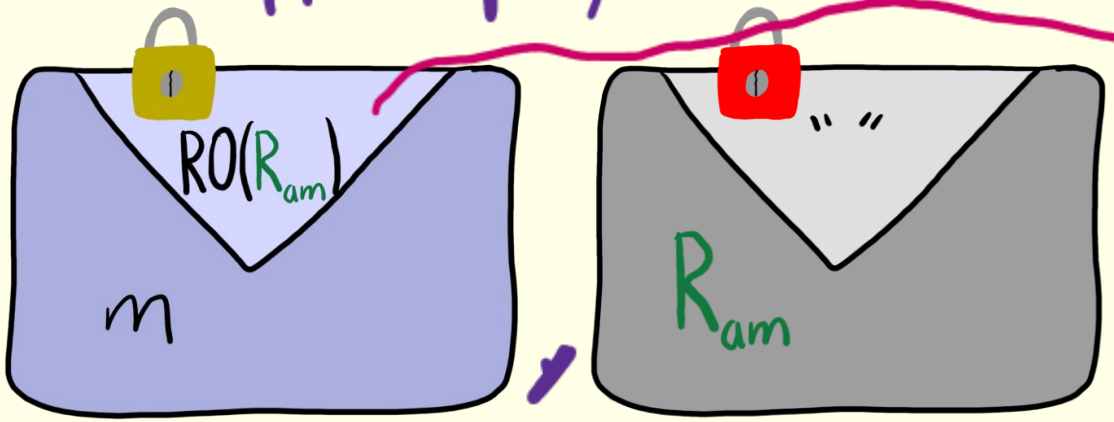


Final Construction

$Enc(pp, pk, m; R) =$



$AEnc(pp, pk, ak, m, am) =$



only info on am, $< \log \lambda$ bits of info

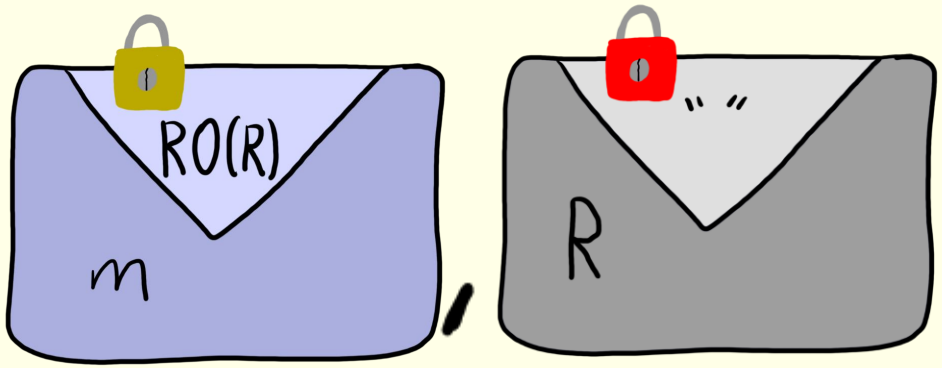
Dictatoria ~~ARE~~ in ROM

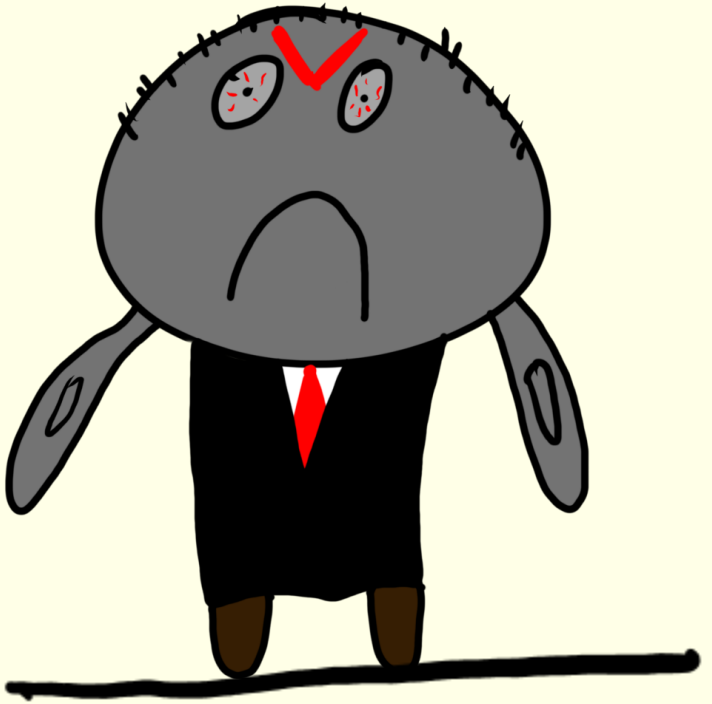
universal backdoor.

Dictator can read all messages & detect anamorphism <u>without</u> secret-key access

Dictatoria

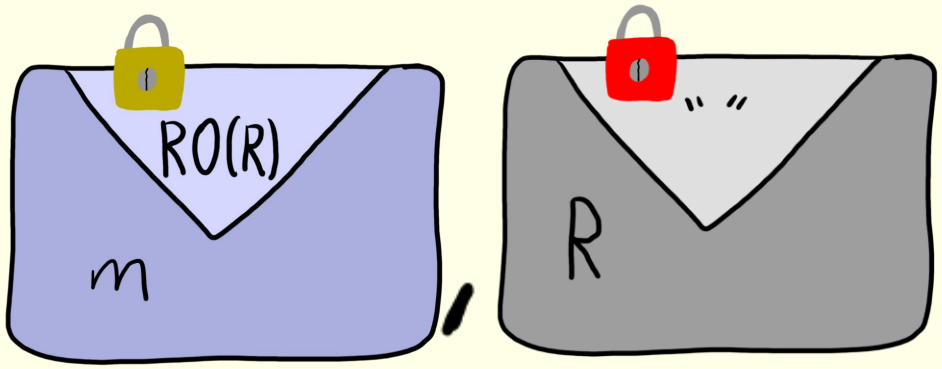
ARE

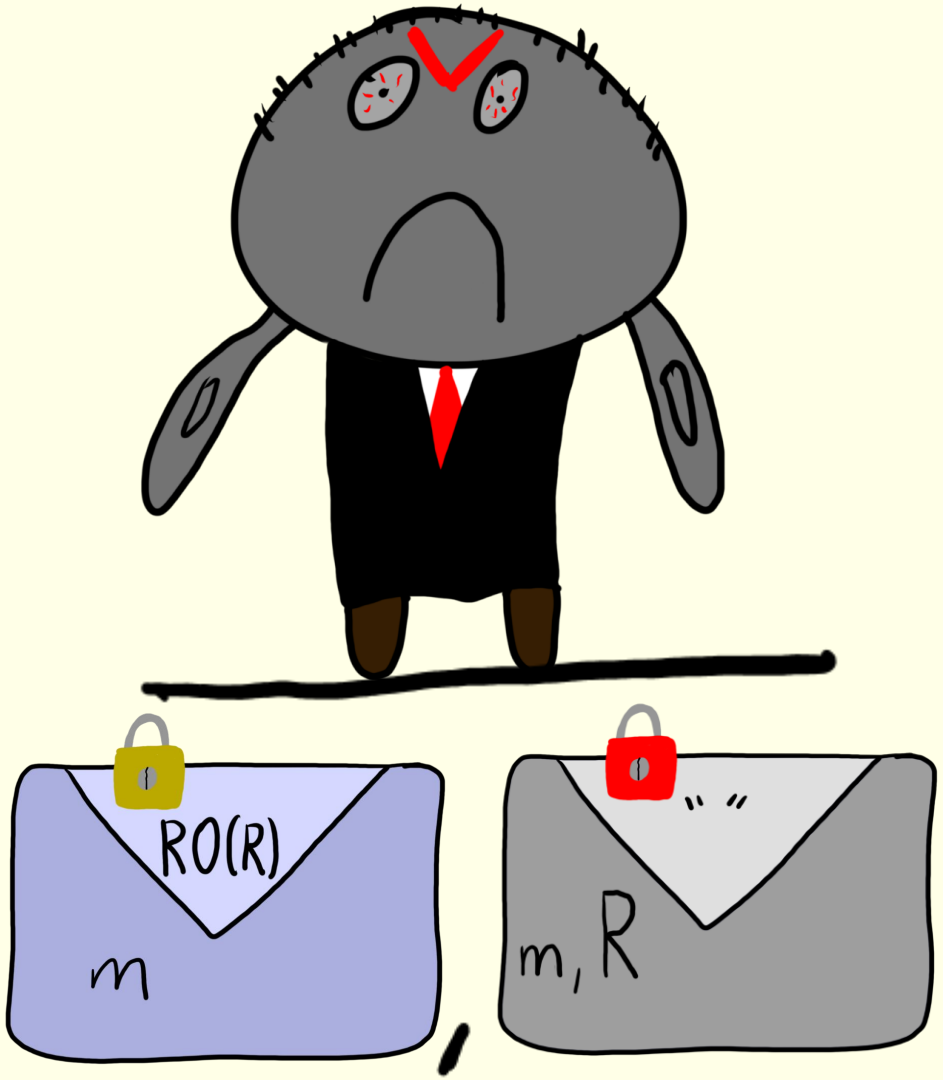




Dictatoria

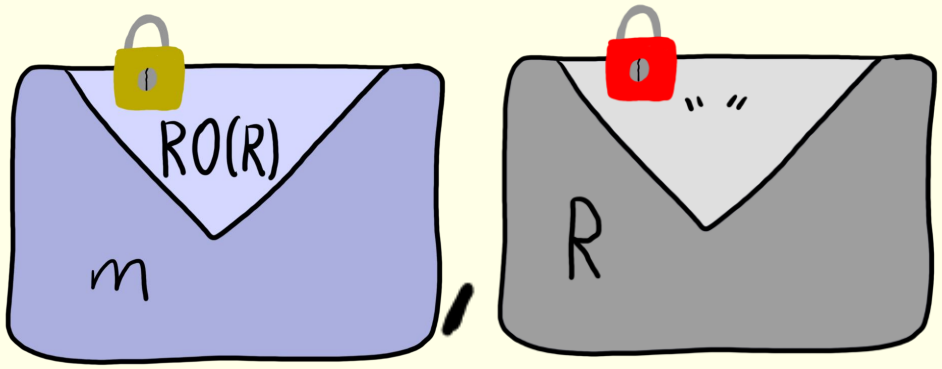
ARE

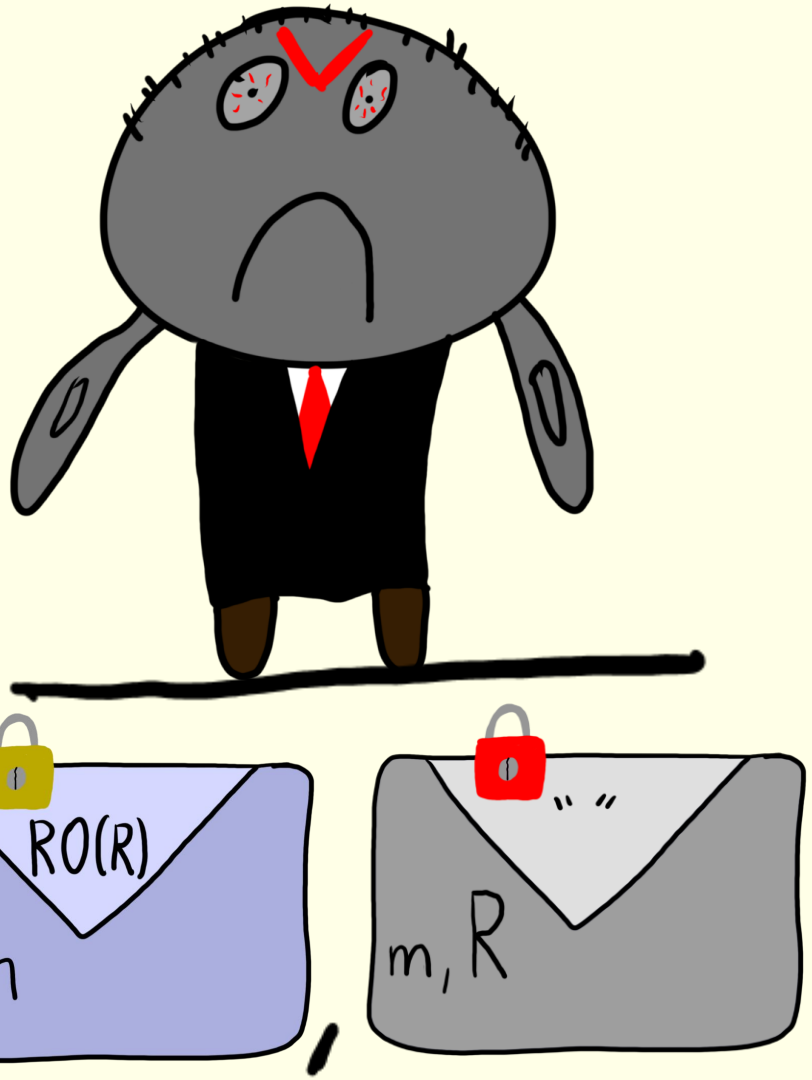




Dictatoria

ARE





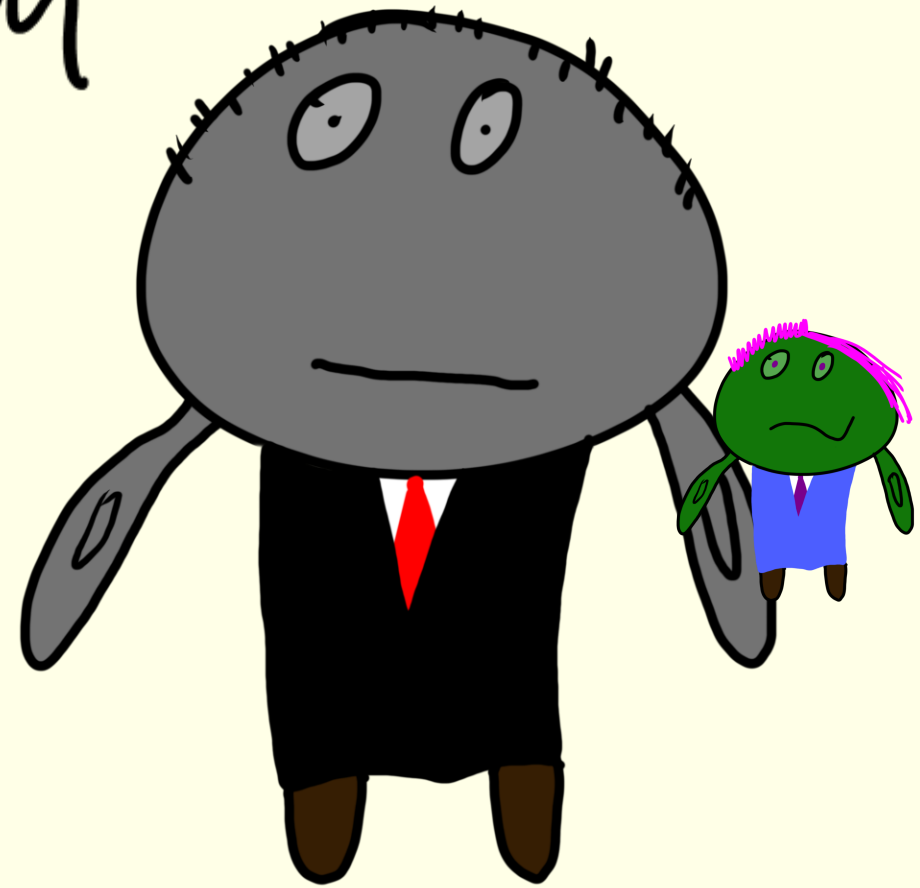
Dictator can read all m to detect covert messages

Warrantland in ROM

ARE which needs secret key access.

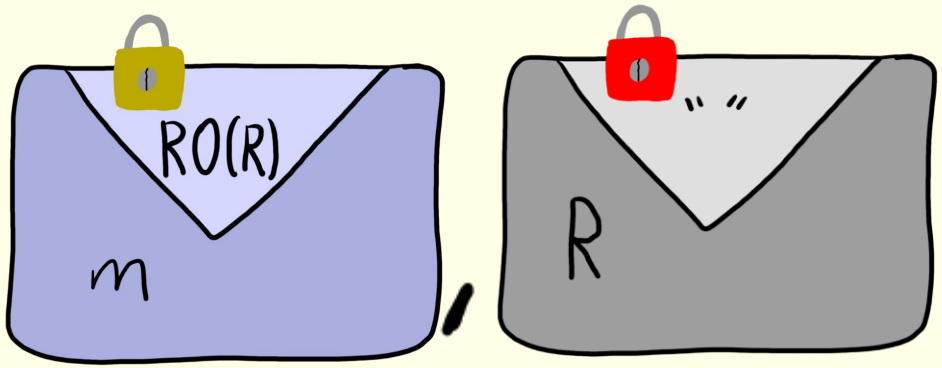
If  hidden, secure against govt. w/ 

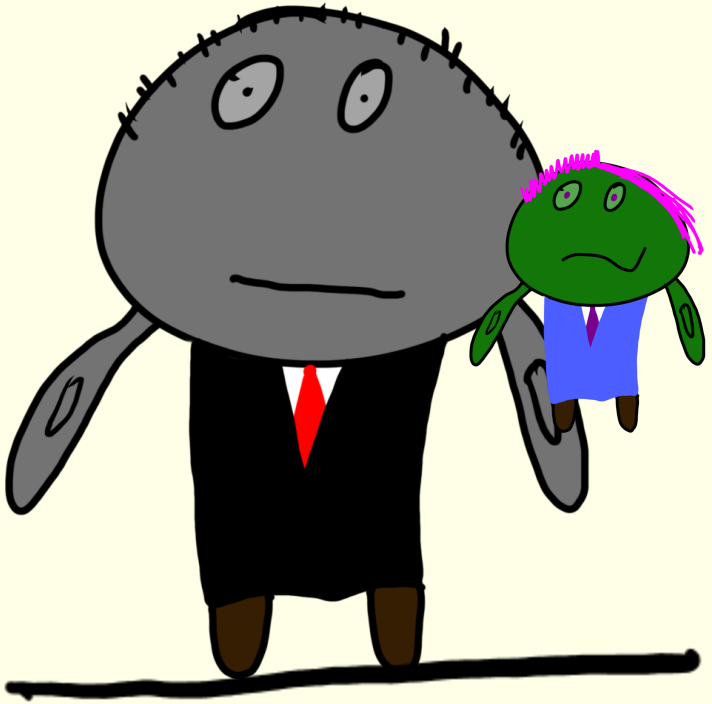
backdoor



Warrantland

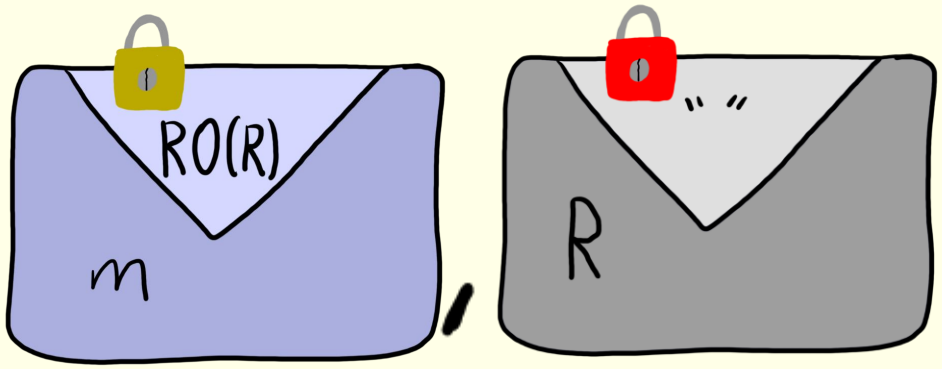
ARE

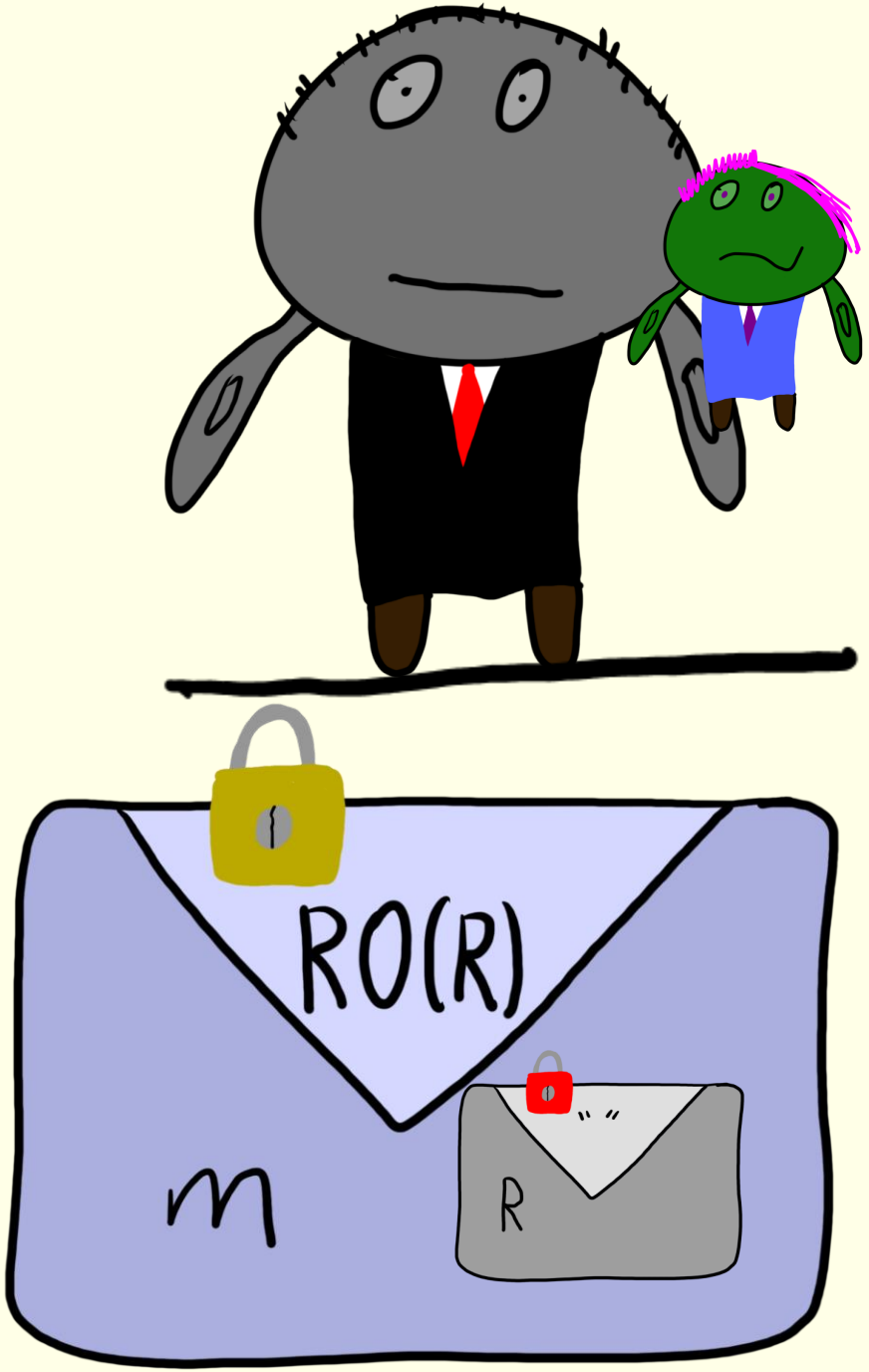




Warrantland

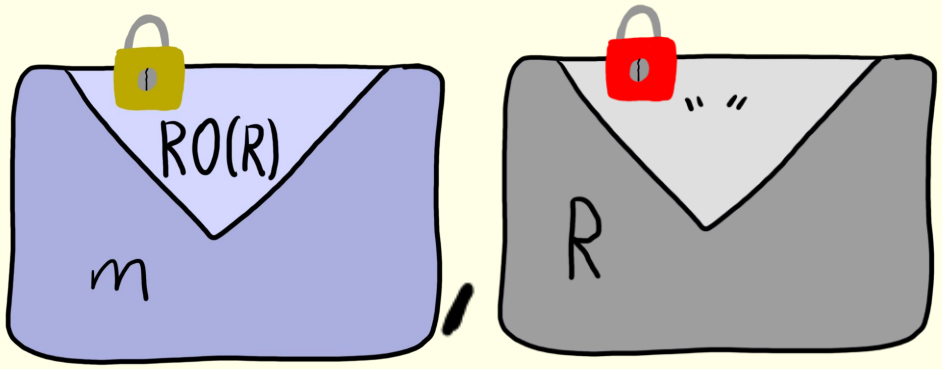
ARE



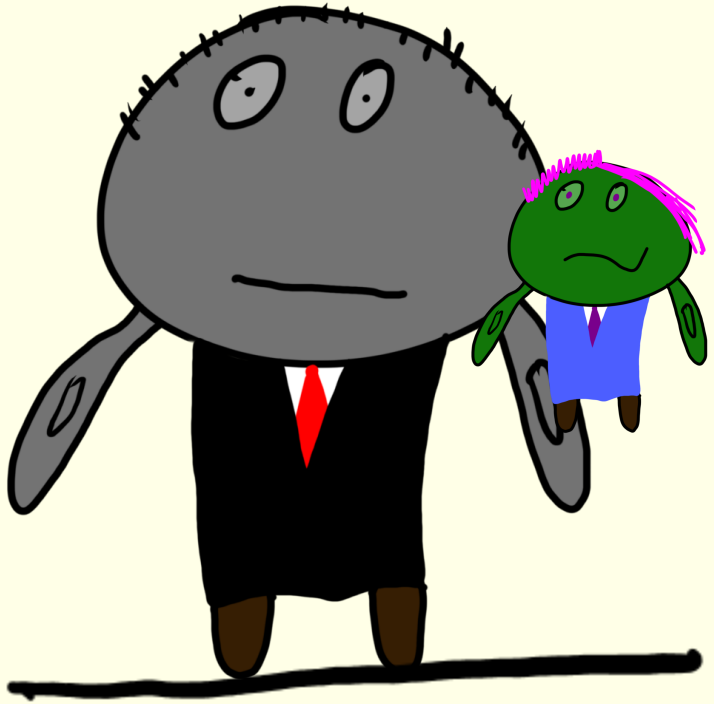


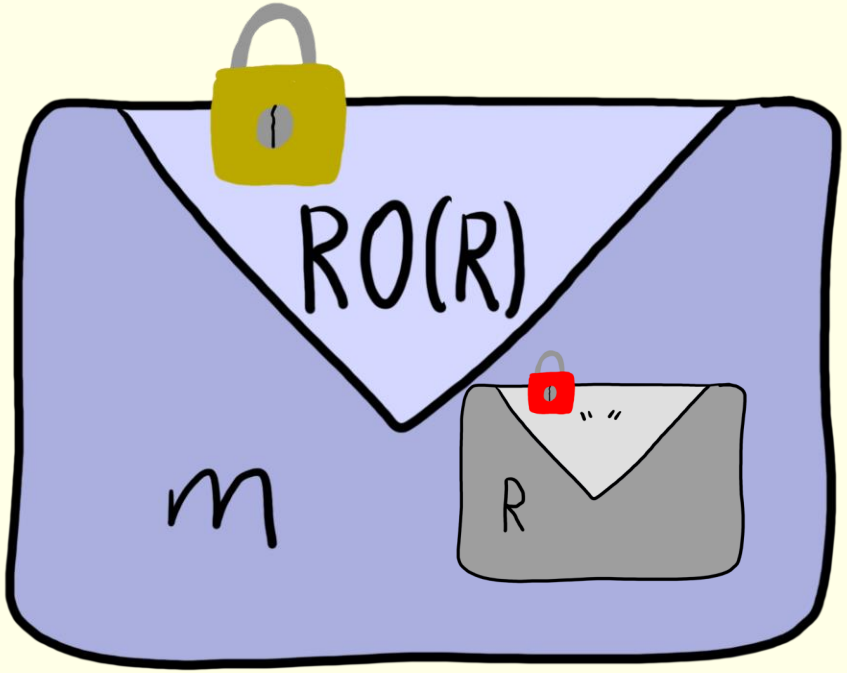
Warrantland

ARE



Govt. needs  to detect anamorphism or break PKE.





Open Questions

1. Standard Model ARE
   [ABG+25] from exponential DDH
2. Getting rid of public parameters.
   [CCGM25] does for weaker notion of ARE
3. Can we bypass this impossibility?
   Is a weaker notion always possible?

Thanks
for
listening!