LVRJHQLHV & LVRPHWULHV

Nulmq Uhlmqghuv - 10.30 - Pdb 12, 2025

LVRJHQLHV & LVRPHWULHV

LVRJHQLHV & LVRPHWULHV

KVRJHQLHV & LVRPHWULHV

JVRJHQLHV & LVRPHWULHV

EFGHIJKLMN

IVRJHQLHV & LVRPHWULHV

QMECLGCQ & GQMKCRPGCQ
ERNFDMHDR & HRNLDSQHDR
FSOGENIES & ISOMETRIES
GTPHFOJFT & JTPNFUSJFT
HUQIGPKGU & KUQOGVTKGU
IVRJHQLHV & LVRPHWULHV
J
K
L
M
N

EQMECLGCQ & GQMKCRPGCQ
FRNFDMHDR & HRNLDSQHDR
GSOGENIES & ISOMETRIES
HTPHFOJFT & JTPNFUSJFT
IUQIGPKGU & KUQOGVTKGU
JVRJHQLHV & LVRPHWULHV
K
L
M
N

EPLDBKFBP & FPLJBQOFBP
FQMECLGCQ & GQMKCRPGCQ
GRNFDMHDR & HRNLDSQHDR
HSOGENIES & ISOMETRIES
ITPHFOJFT & JTPNFUSJFT
JUQIGPKGU & KUQOGVTKGU
KVRJHQLHV & LVRPHWULHV
LWSKIRMIW & MWSQIWUIW
MXTLJSNJX & NXTRJXVJX

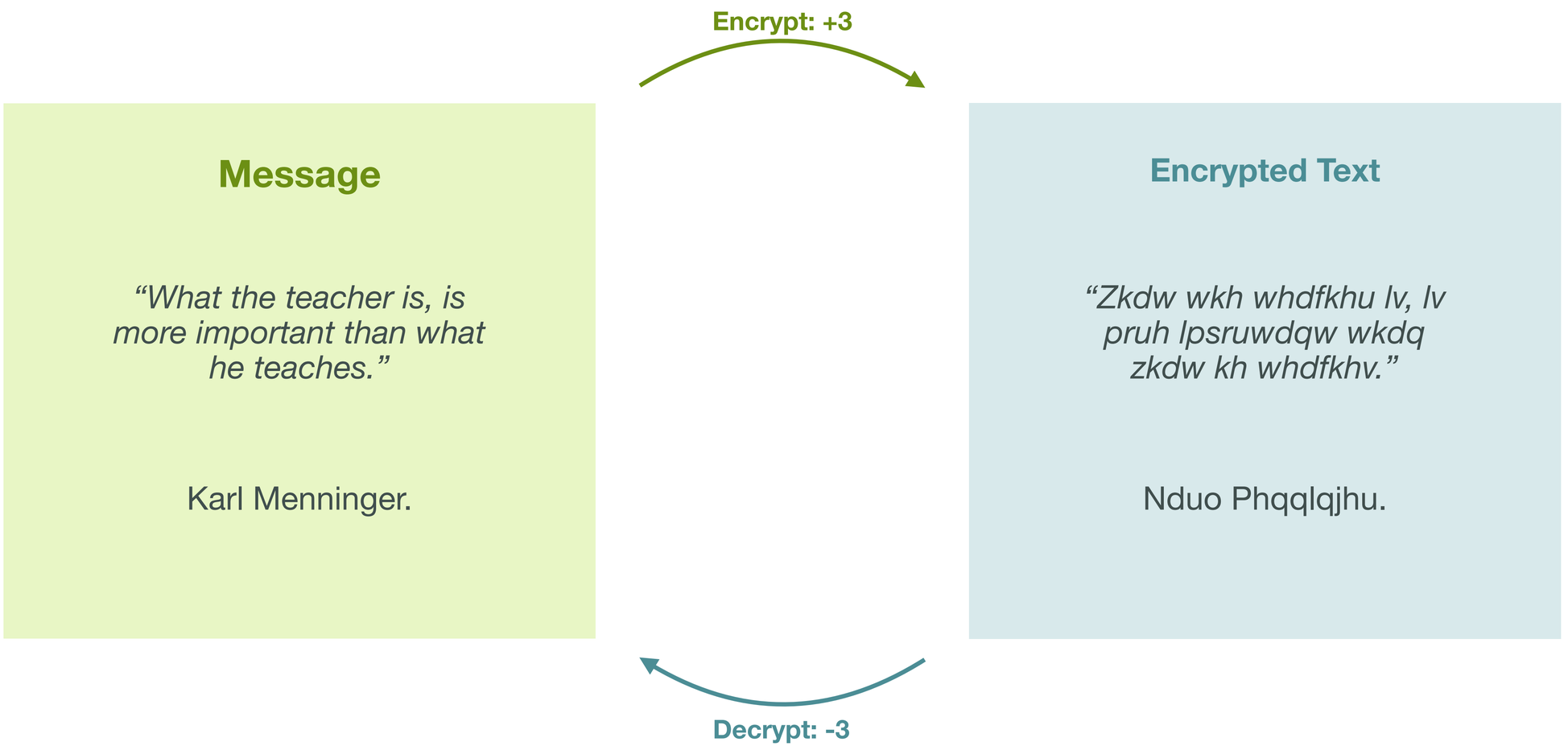
ISOGENIES & ISOMETRIES

ISOGENIES & ISOMETRIES

ISOGENIES & ISOMETRIES

Krijn Reijnders - 10.30 - May 12, 2025

Our First Encryption!



(Diffie and Hellman, 1976)

MESSAGE: `Innovation […] has come primarily from the amateurs`

KEYWORD: `crypto`
(repeats)

(Diffie and Hellman, 1976)

MESSAGE: `Innovation […] has come primarily from the amateurs`

KEYWORD: (repeats) **`crypto`**`cryp […] toc rypt ocryptocr ypto cry ptocrypt`

(Diffie and Hellman, 1976)

MESSAGE: Innovation […] has come primarily from the amateurs

09

KEYWORD: **crypto**cryp […] toc rypt ocryptocr ypto cry ptocrypt

(repeats)

03

12

L

(Diffie and Hellman, 1976)

MESSAGE: Innovation […] has come primarily from the amateurs

09 14 14 15 22 01 20 09 15 14 […] 08 01 19 03 15 13 05 16 18 09 13 01 18 09 12 25 06 18 15 13 20 08 05 01 13 01 20 05 21 18 19

KEYWORD: **crypto**cryp […] toc rypt ocryptocr ypto cry ptocrypt

(repeats)

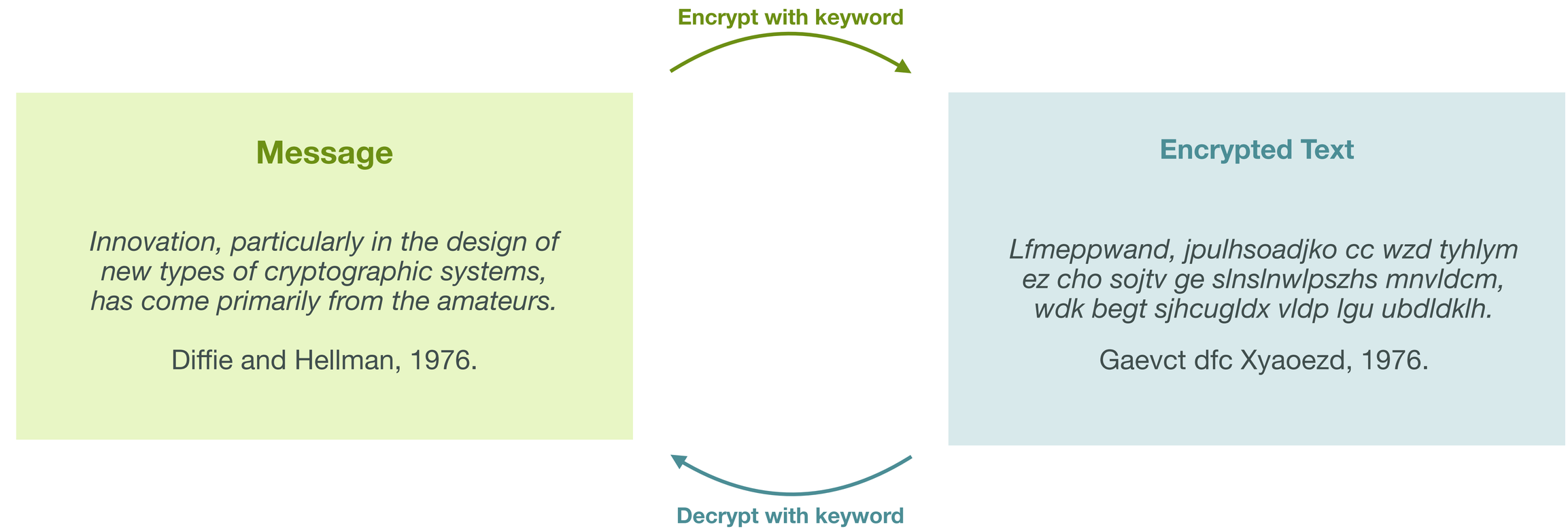
03 18 25 16 20 15 03 18 25 16 […] 20 15 03 18 25 16 20 15 03 18 25 16 20 15 03 18 25 16 20 15 03 18 25 16 20

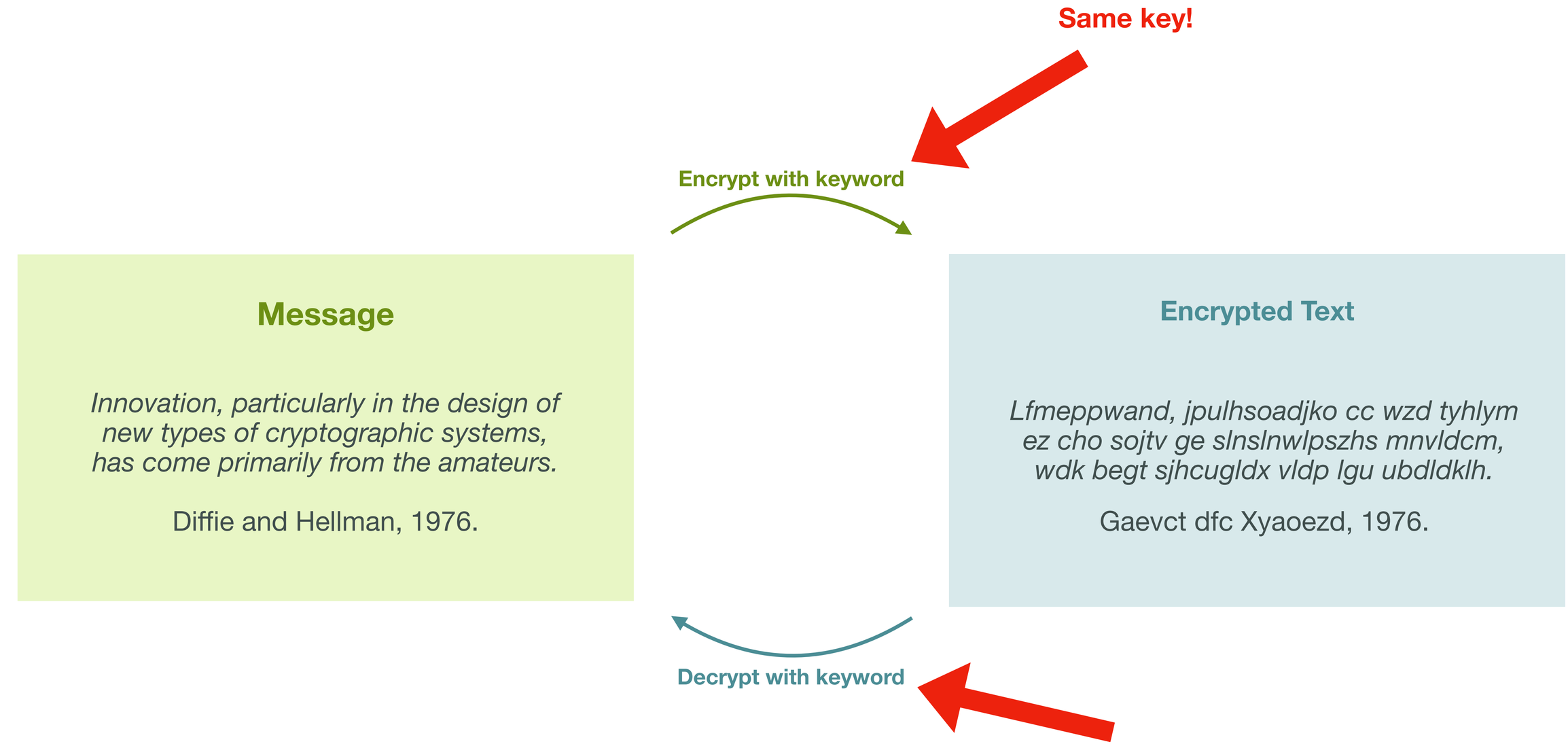
---

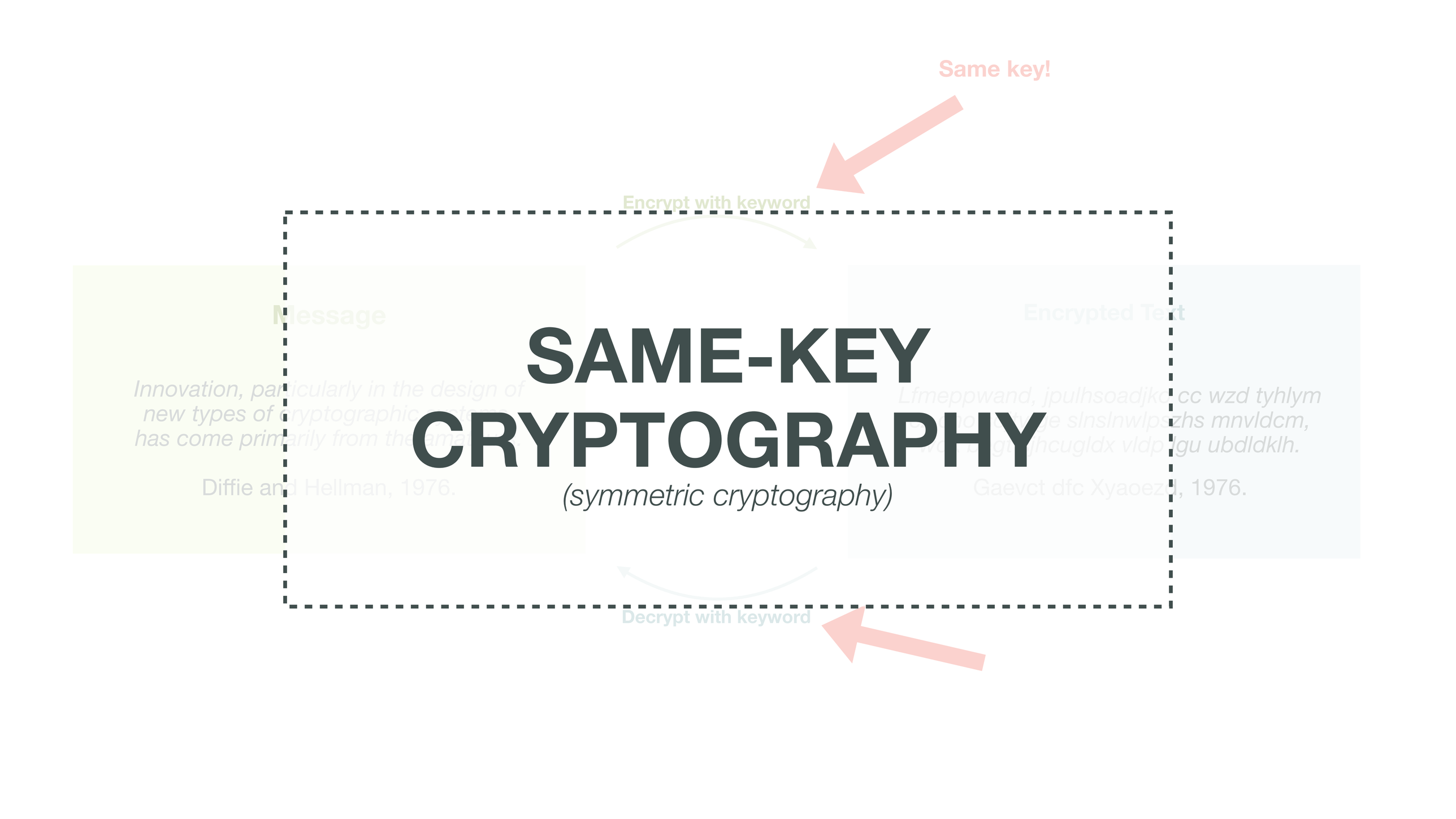
12 06 13 05 16 16 23 01 14 04 […] 02 06 22 21 14 03 25 05 21 01 12 17 12 24 15 17 05 08 09 02 23 26 04 17 07 16 23 23 20 08 13

ENCRYPTION: Lfmeppwand […] bpv uncy eualqlxoq ehib wzd qgpwwthm

Vigenère Encryption!

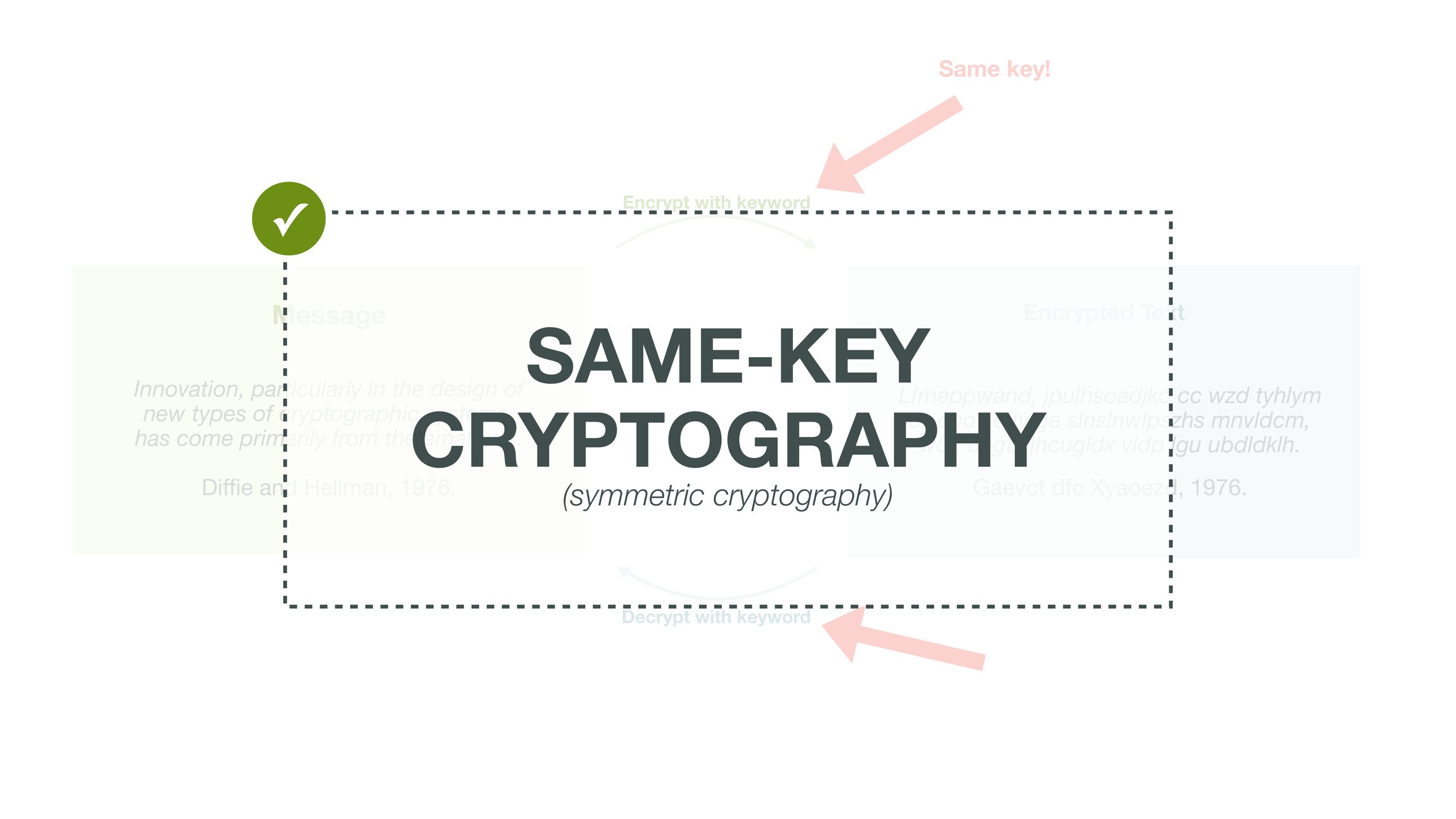



Same key!
Encrypt with keyword
Message
Innovation, particularly in the design of new types of cryptographic systems, has come primarily from the amateurs.
Diffie and Hellman, 1976.
Encrypted Text
Lfmeppwand, jpulhsoadjko cc wzd tyhlym ez cho sojtv ge slnslnwlpszhs mnvldcm, wdk begt sjhcugldx vldp lgu ubdldklh.
Gaevct dfc Xyaoezd, 1976.
Decrypt with keyword



SAME-KEY CRYPTOGRAPHY

(symmetric cryptography)



SAME-KEY CRYPTOGRAPHY

(symmetric cryptography)

Encrypt with my *public* lock

Message

Innovation, particularly in the design of new types of cryptographic systems, has come primarily from the amateurs.

Diffie and Hellman, 1976.

Encrypted Text

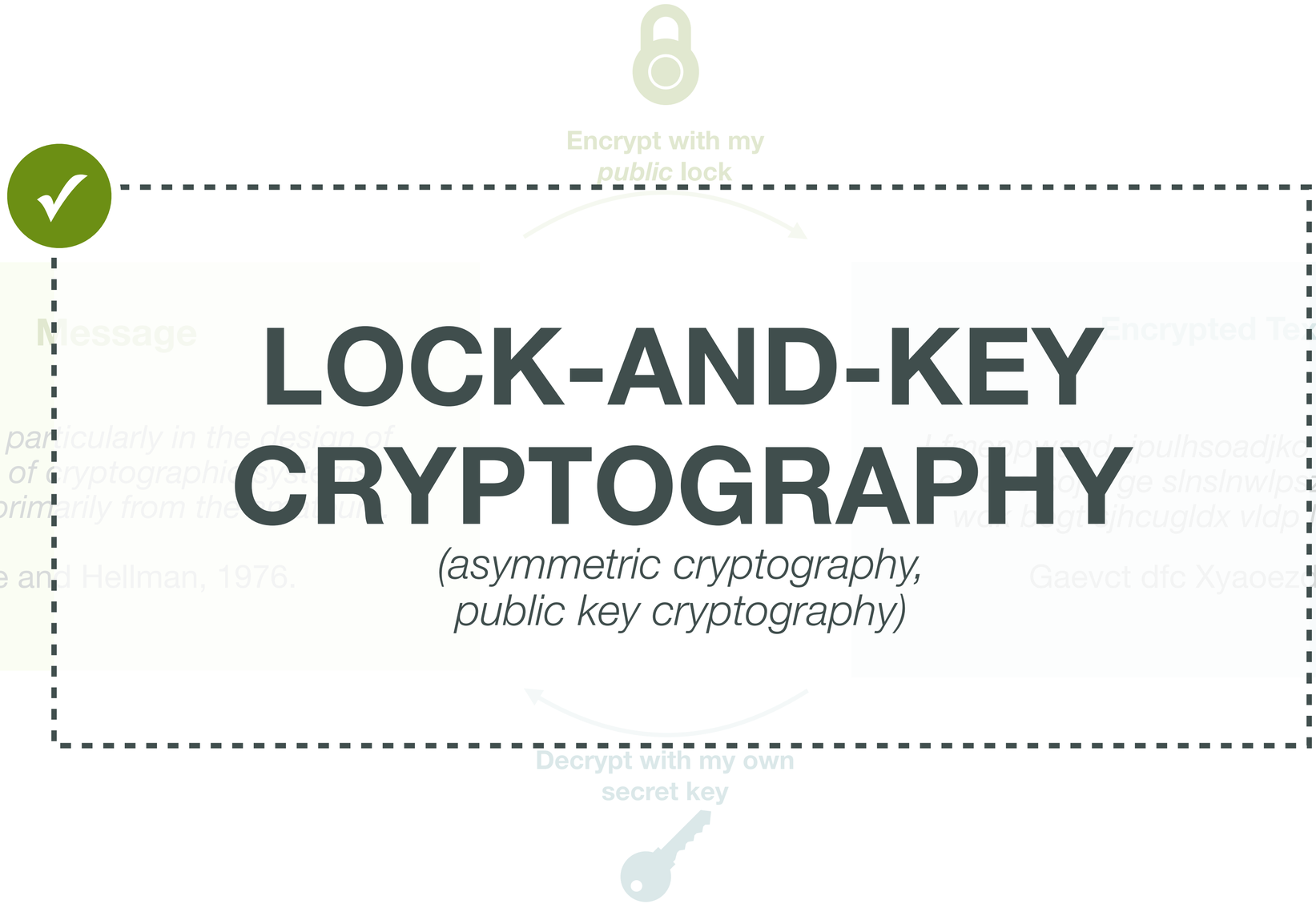
Lfmeppwand, jpulhsoadjko cc wzd tyhlym ez cho sojtv ge slnslnwlpszhs mnvldcm, wdk begt sjhcugldx vldp lgu ubdldklh.

Gaevct dfc Xyaoezd, 1976.

Decrypt with my own secret key

LOCK-AND-KEY CRYPTOGRAPHY

(asymmetric cryptography,
public key cryptography)



LOCK-AND-KEY CRYPTOGRAPHY

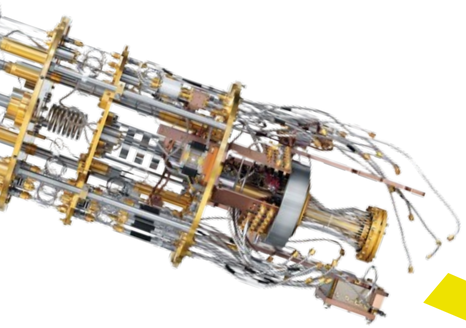
(asymmetric cryptography, public key cryptography)

SAME-KEY CRYPTOGRAPHY

(symmetric cryptography)

LOCK-AND-KEY CRYPTOGRAPHY

(asymmetric cryptography, public key cryptography)

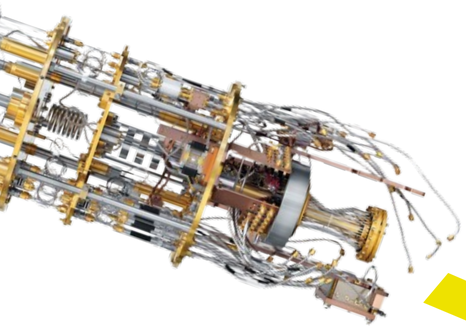


SAME-KEY CRYPTOGRAPHY

(symmetric cryptography)

LOCK-AND-KEY CRYPTOGRAPHY

(asymmetric cryptography, public key cryptography)



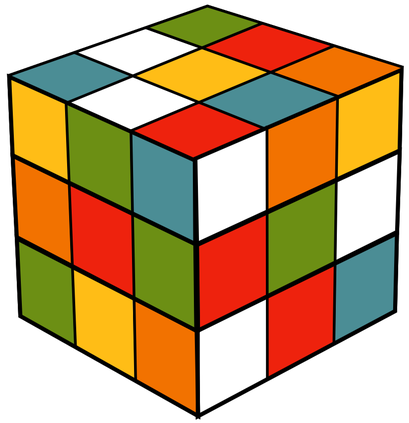
SAME-KEY CRYPTOGRAPHY

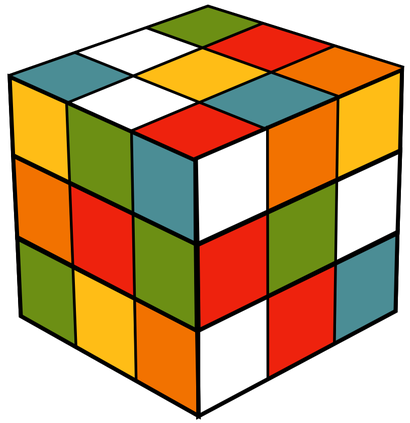
(symmetric cryptography)

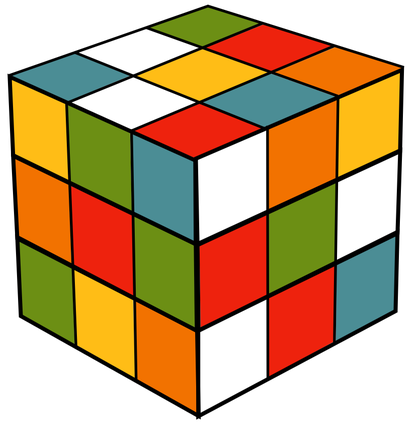
POST-QUANTUM CRYPTOGRAPHY

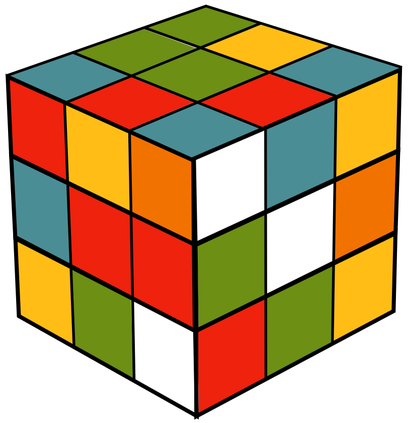
ISOGENIES & ISOMETRIES

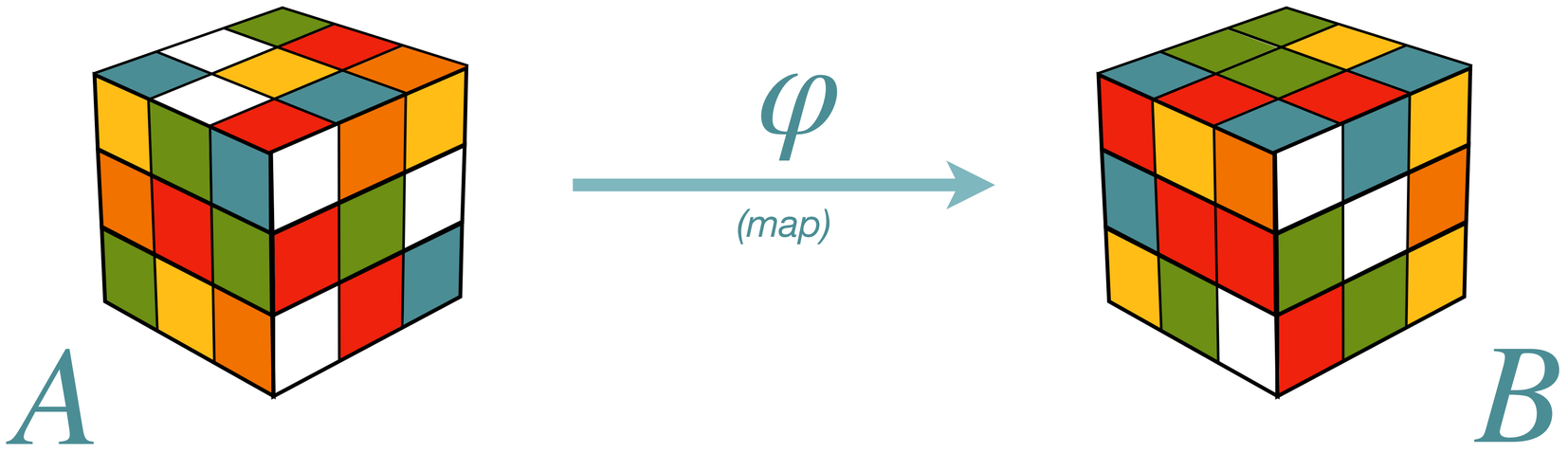
Krijn Reijnders - 10.30 - May 12, 2025

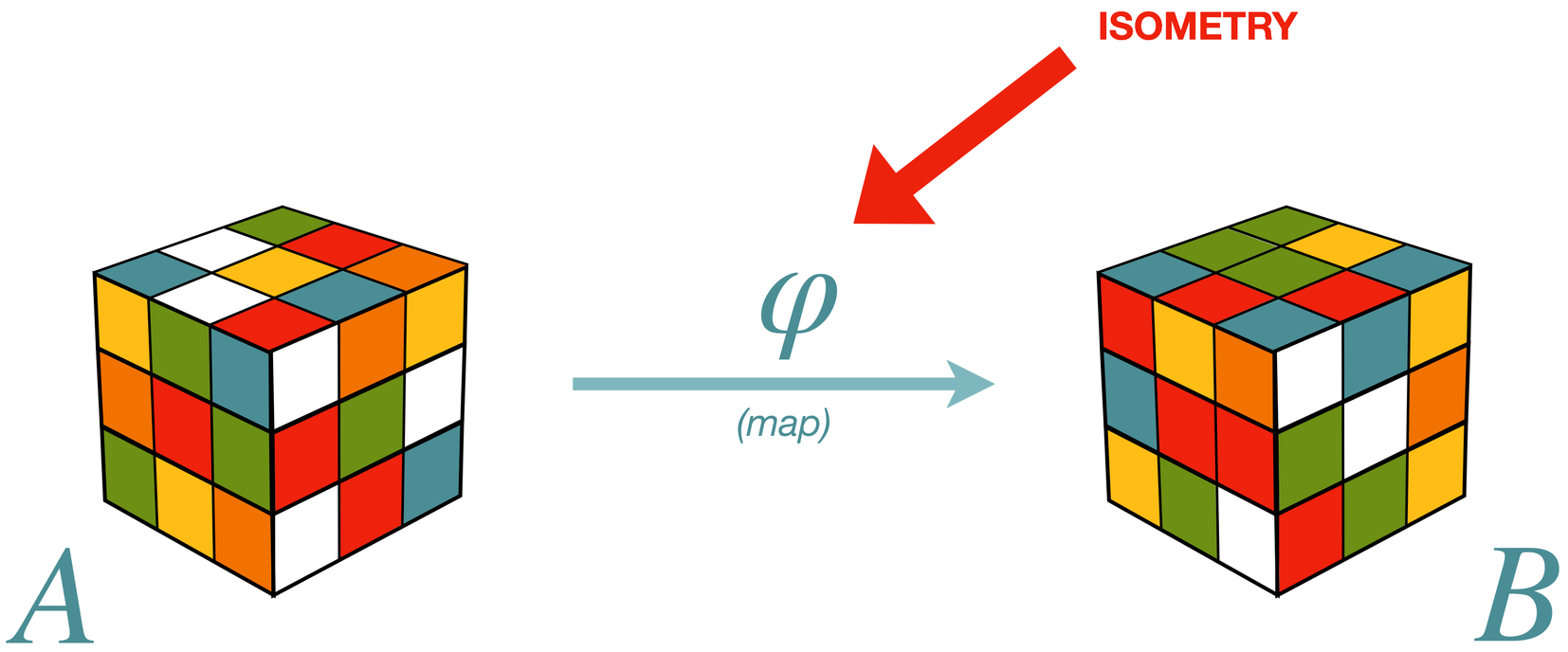


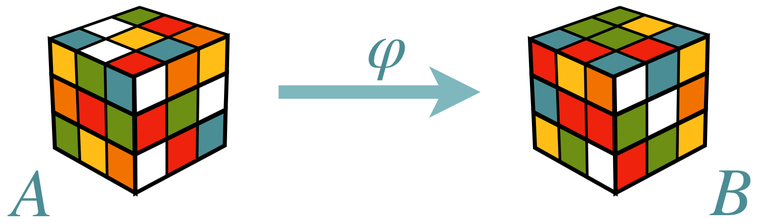







A
φ
(map)
B


ISOMETRY
φ
(map)
A
B

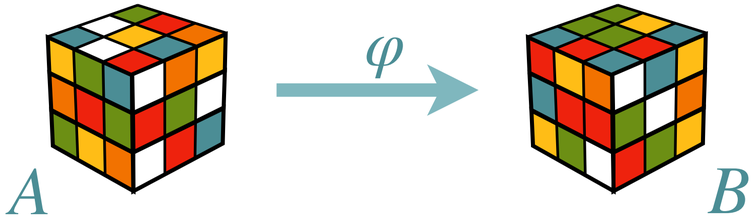


analysis

Understanding
these maps

design

Build cryptography
from these maps



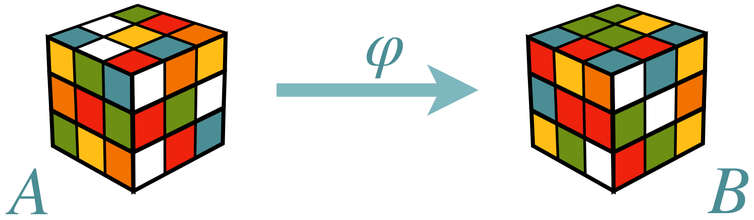
analysis

Understanding
these maps

- if we know the objects A and B, how **hard** is it to find the map φ ?
- if we have a **quantum computer**, is it easier to find the map φ ?
- when we compute φ in practice, do we **leak information** on φ ?

design

Build cryptography
from these maps



analysis

Understanding
these maps

- if we know the objects A and B, how **hard** is it to find the map φ ?
- if we have a **quantum computer**, is it easier to find the map φ ?
- when we compute φ in practice, do we **leak information** on φ ?

design

Build cryptography
from these maps

- how **versatile** is cryptography using these type of maps φ ?
- how **efficient** is cryptography using these type of maps φ ?
- can we use **smarter maths** to compute φ more efficiently?

	ISOGENIES	ISOMETRIES
analysis		
design		

	ISOGENIES	ISOMETRIES
analysis	**Chapter 4** if you **listen carefully** to your chip, you can learn secret isogenies	
design		

	ISOGENIES	ISOMETRIES
analysis	Chapter 4 if you **listen carefully** to your chip, you can learn secret isogenies Chapter 5 if you **shoot lasers** at your chip, you can learn secret isogenies	
design		

	ISOGENIES	ISOMETRIES
analysis	**Chapter 4** if you **listen carefully** to your chip, you can learn secret isogenies **Chapter 5** if you **shoot lasers** at your chip, you can learn secret isogenies	
design	**Chapter 6 & 8** using **smarter maths** makes certain isogenies faster and safer	

	ISOGENIES		ISOMETRIES
analysis	**Chapter 4** if you **listen carefully** to your chip, you can learn secret isogenies	**Chapter 5** if you **shoot lasers** at your chip, you can learn secret isogenies	
design	**Chapter 6 & 8** using **smarter maths** makes certain isogenies faster and safer	**Chapter 7** if you make everything **super safe** for isogenies, it all becomes very slow	

	ISOGENIES	ISOMETRIES
analysis	**Chapter 4** if you **listen carefully** to your chip, you can learn secret isogenies **Chapter 5** if you **shoot lasers** at your chip, you can learn secret isogenies	
design	**Chapter 6 & 8** using **smarter maths** makes certain isogenies faster and safer **Chapter 7** if you make everything **super safe** for isogenies, it all becomes very slow **Chapter 9 & 10** we can make certain isogenies **much faster**, if we make others slow	

	ISOGENIES	ISOMETRIES
analysis	**Chapter 4** if you **listen carefully** to your chip, you can learn secret isogenies **Chapter 5** if you **shoot lasers** at your chip, you can learn secret isogenies	
design	**Chapter 6 & 8** using **smarter maths** makes certain isogenies faster and safer **Chapter 7** if you make everything **super safe** for isogenies, it all becomes very slow **Chapter 9 & 10** we can make certain isogenies **much faster**, if we make others slow **Chapter 11** using more complex maths makes some isogenies **very cool** but slow	

	ISOGENIES		ISOMETRIES
analysis	**Chapter 4** if you **listen carefully** to your chip, you can learn secret isogenies	**Chapter 5** if you **shoot lasers** at your chip, you can learn secret isogenies	**Chapter 12** our **new algorithm** finds secret isometries faster, but its still very hard
design	**Chapter 6 & 8** using **smarter maths** makes certain isogenies faster and safer	**Chapter 7** if you make everything **super safe** for isogenies, it all becomes very slow	
	Chapter 9 & 10 we can make certain isogenies **much faster**, if we make others slow	**Chapter 11** using more complex maths makes some isogenies **very cool** but slow	

	ISOGENIES		ISOMETRIES
analysis	**Chapter 4** if you **listen carefully** to your chip, you can learn secret isogenies	**Chapter 5** if you **shoot lasers** at your chip, you can learn secret isogenies	**Chapter 12** our **new algorithm** finds secret isometries faster, but its still very hard
design	**Chapter 6 & 8** using **smarter maths** makes certain isogenies faster and safer	**Chapter 7** if you make everything **super safe** for isogenies, it all becomes very slow	**Chapter 13** we make **digital signatures** from isometries, but… they're slow and big
	Chapter 9 & 10 we can make certain isogenies **much faster**, if we make others slow	**Chapter 11** using more complex maths makes some isogenies **very cool** but slow	

	ISOGENIES	ISOMETRIES
analysis	**Chapter 4** if you **listen carefully** to your chip, you can learn secret isogenies **Chapter 5** if you **shoot lasers** at your chip, you can learn secret isogenies	**Chapter 12** our **new algorithm** finds secret isometries faster, but its still very hard
design	**Chapter 6 & 8** using **smarter maths** makes certain isogenies faster and safer **Chapter 7** if you make everything **super safe** for isogenies, it all becomes very slow **Chapter 9 & 10** we can make certain isogenies **much faster**, if we make others slow **Chapter 11** using more complex maths makes some isogenies **very cool** but slow	**Chapter 13** we make **digital signatures** from isometries, but… they're slow and big **Chapter 14** you can use maths to make these signatures **smaller and faster**

	ISOGENIES		ISOMETRIES	
analysis	**Chapter 4** if you **listen carefully** to your chip, you can learn secret isogenies	**Chapter 5** if you **shoot lasers** at your chip, you can learn secret isogenies	**Chapter 12** our **new algorithm** finds secret isometries faster, but its still very hard	
design	**Chapter 6 & 8** using **smarter maths** makes certain isogenies faster and safer	**Chapter 7** if you make everything **super safe** for isogenies, it all becomes very slow	**Chapter 13** we make **digital signatures** from isometries, but… they're slow and big	**Chapter 14** you can use maths to make these signatures **smaller and faster**
	Chapter 9 & 10 we can make certain isogenies **much faster**, if we make others slow	**Chapter 11** using more complex maths makes some isogenies **very cool** but slow		

ISO → GE

METR → IE

SO → GEN

METR → IES

1

Certain cryptography made from isogenies (CSIDH) is now faster and more secure, but **not yet ready** for the real world.

1

Certain cryptography made from isogenies (CSIDH) is now faster and more secure, but **not yet ready** for the real world.

2

Other cryptography made from isogenies (SQIsign) is now faster and more secure, and looks **pretty promising** for the future!

1

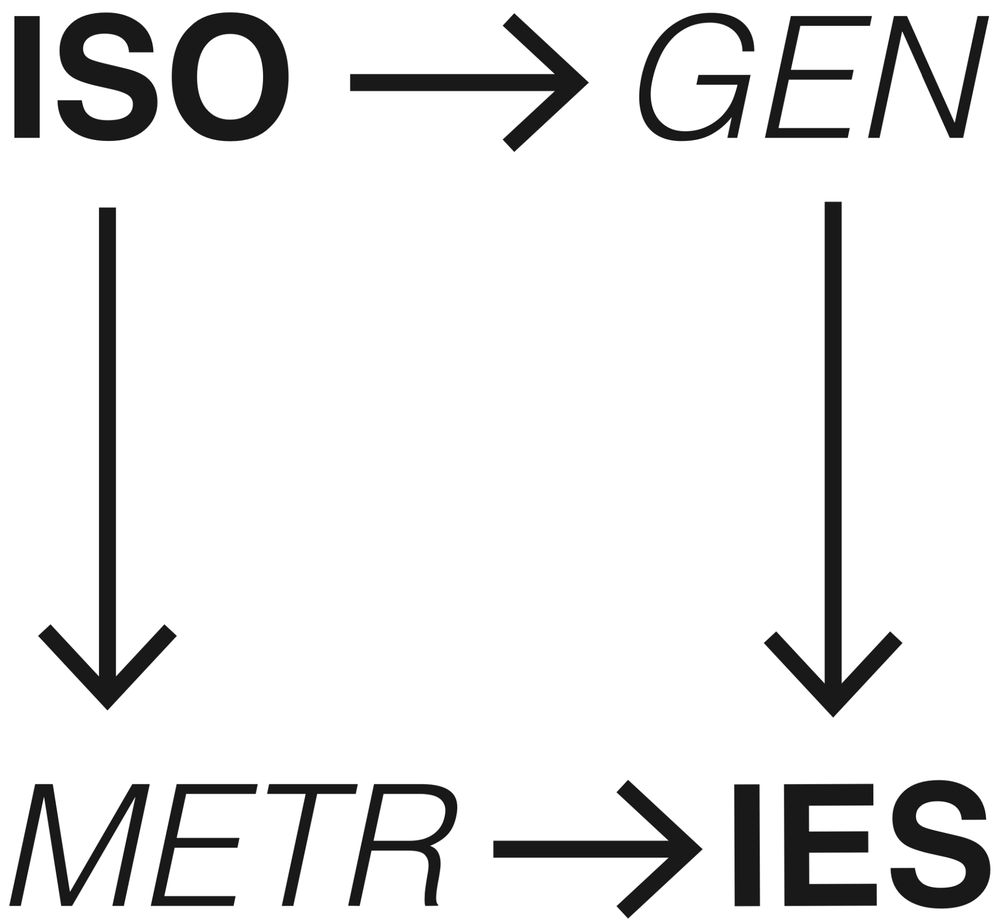
Certain cryptography made from isogenies (CSIDH) is now faster and more secure, but **not yet ready** for the real world.

2

Other cryptography made from isogenies (SQIsign) is now faster and more secure, and looks **pretty promising** for the future!

3

Our cryptography made from isometries (MCE) is a nice try, but has **major issues**…
We should be more bold with isometries!


ISO → GEN
METR → IES