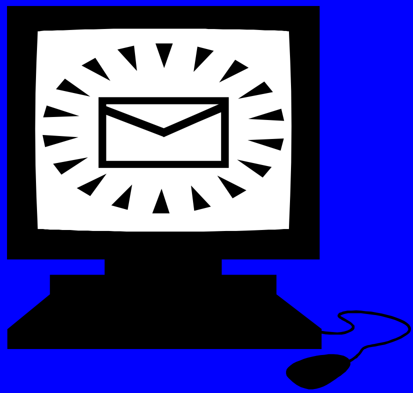
Cryptography and Pseudorandomness



Theoretical ideas behind e-commerce and the Internet revolution

Avi Wigderson
Institute for Advanced Study

Plan

- Cryptography before computational complexity
- The ambitions of modern cryptography
- The assumptions of modern cryptography
- The “digital envelope” abstraction

Blackboard break: Formalizing some of the defs. Psudorandomness, and modern broader context. Hardness amplification proof.

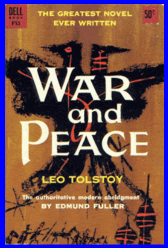
- Zero-knowledge proofs

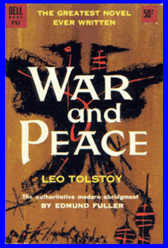
Cryptography before 1970s

Alice

Secret communication

Bob



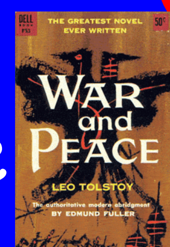


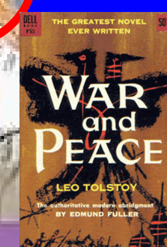
Assumes Alice and Bob share
Information which no one else has

Secret communication since 1970s

Alice and Bob want to have a completely private conversation.

They share no private information





Many in this audience has already faced and solved this problem often!

I want to purchase "War and Peace". My credit card is number is 1111 2222 3333 4444

Public-key encryption, e-commerce security

Diffie-Hellman, Merkle, Rivest-Shamir-Adleman, Rabin 1976-77

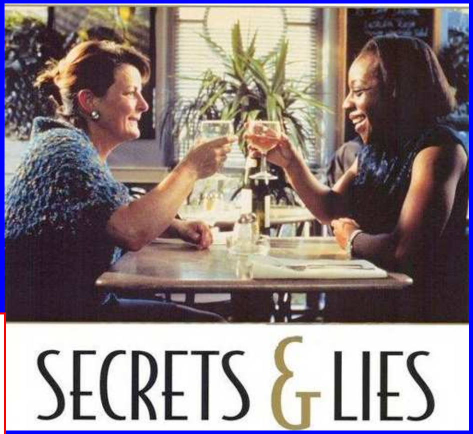
Key conceptual ideas: complexity-based crypto, one-way and trapdoor functions

Goldwasser-Micali, Blum-Micali, Yao 1981

Key formal definitions, techniques and proofs: Computational indistinuishability, pseudorandomness

Modern Cryptography

Any task with conflict between privacy and resilience.



Mathematics of

- Encryption
- Identification
- Money transfer
- Public bids
- Secret exchange
- Poker game on the phone
- Public lottery
- Sign contracts

Digitally, with no trusted parties

Mostly developed before the Internet

What are we assuming?

Axiom 1: Agents are computationally limited (say, to polynomial time)

Consequence 1: Only tasks having efficient algorithms can be performed

Easy and Hard Problems

asymptotic complexity of functions

Multiplication

mult(23,67) = 1541

grade school algorithm:

n^2 steps on n digit inputs

EASY

Can be performed quickly for huge integers

Factoring

factor(1541) = (23,67)

best known algorithm:

$\exp(\sqrt{n})$ steps on n digits

HARD?

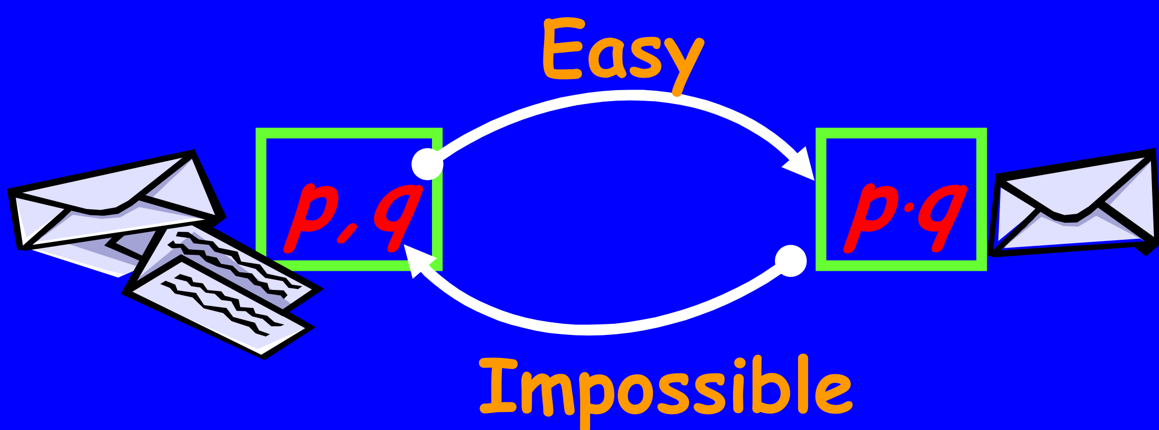
We don't know!

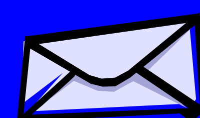
We'll assume it.

Axiom 2: Factoring is hard!

Axiom 1: Agents are computationally limited

Axiom 2: Factoring is hard



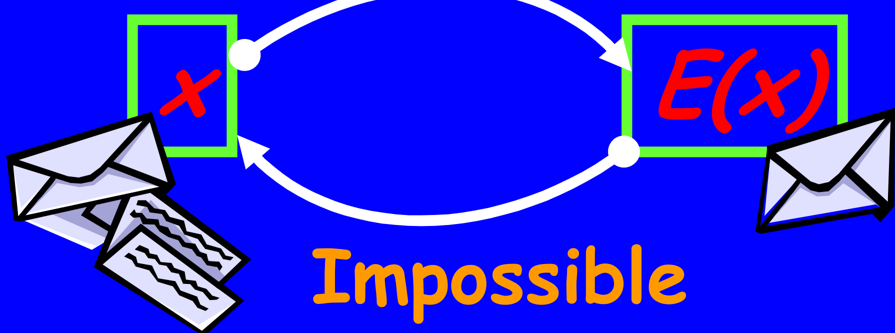
Theorem: Axioms $\Rightarrow$ digital 

One-way functions

Axiom 1: Agents are computationally limited

Axiom 2': The exist one-way functions E

Easy



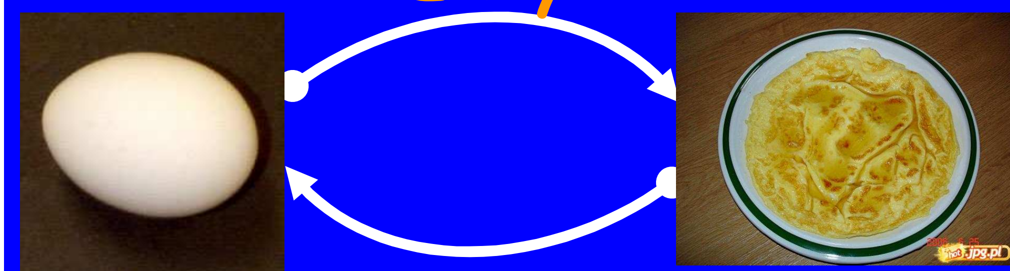
Impossible

Example: $E(p,q) = p \cdot q$

E is multiplication

We have other E's

Easy



Impossible

Nature's one-way functions: 2nd law of Thermodynamics

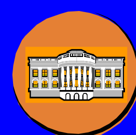
Blum
1981

Envelopes as commitments

Alice

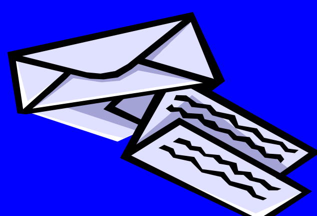
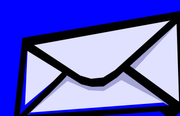
if  I get the car (else you do)

Bob

flipping...  What did you pick?

---

x *E(x)*

OPEN   CLOSED

- Alice can insert any *x* (even 1 bit)
- Bob cannot compute content (even partial info)
- Alice cannot change content (*E(x)* defines *x*)
- Alice can prove to Bob that *x* is the content

Intermission –

Switching to a black board lecture

- Formal definititions of computational pseudorandomness.
- Connections and generalizations of these defs to arithmetic combinatorics.
- Using these defs to define digital envelope (formally, a bit-commitment scheme)

Survey by Salil Vadhan:

http://people.seas.harvard.edu/~salil/pseudorandomness/

Zero-knowledge proofs

Copyrights

Dr. Alice: I can prove Riemann's Hypothesis

Prof. Bob: Impossible! What is the proof?

Dr. Alice: Lemma…Proof…Lemma…Proof...

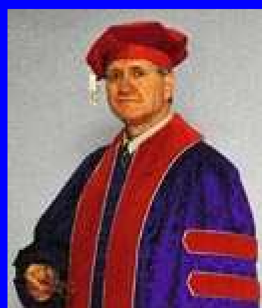
Prof. Bob: ~~Amazing!! I'll recommend tenure~~

Amazing!! I'll publish first

Goldwasser-Micali
-Rackoff 1984

Zero-Knowledge Proof

"Claim"



Bob

Alice ("proof")

Accept/Reject

"Claim" true → Bob accepts
Bob learns nothing*

"Claim" false → Bob rejects with high probability

Goldreich-Micali
-Wigderson 1986

The universality of Zero-Knowledge

Theorem: Everything you can prove at all,
you can prove in Zero-Knowledge

ZK-proofs of Map Coloring

<u>Input</u>: planar map M

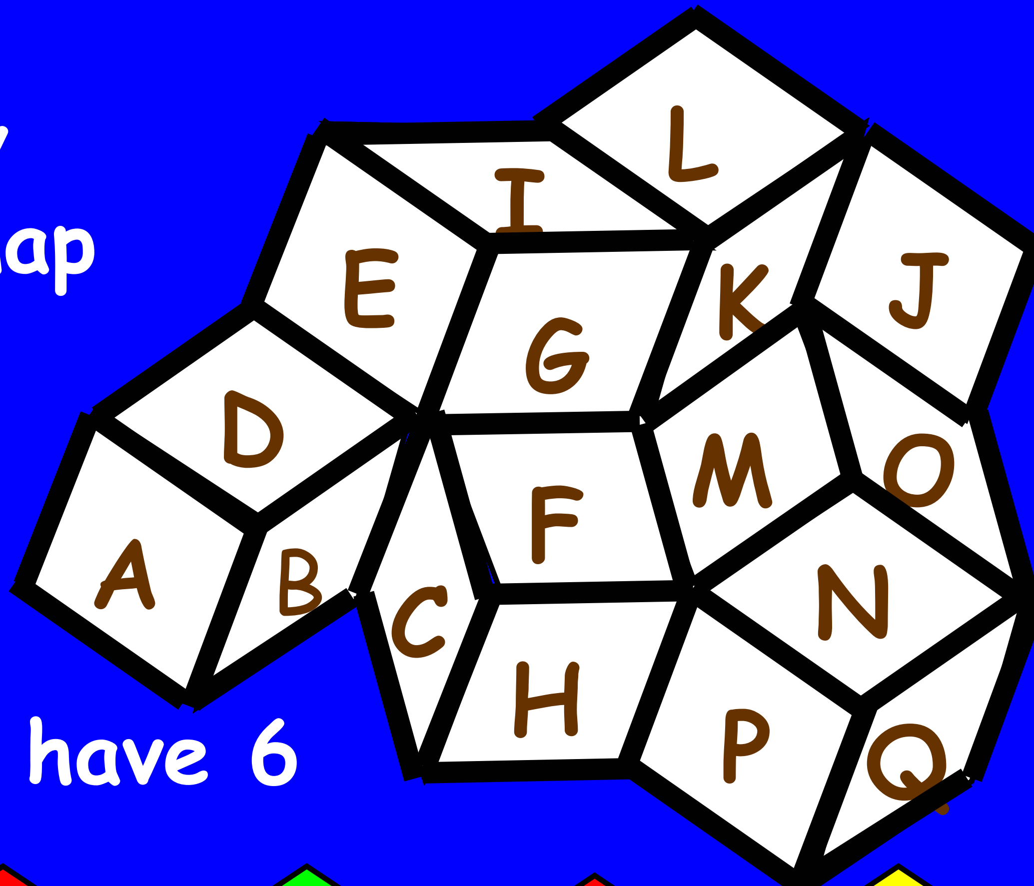
Claim: M is 3-colorable

Natural mathematical
Proof: 3-coloring of M
(gives lots of info)

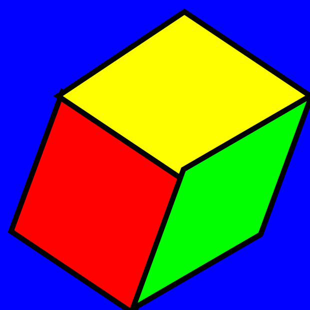
Theorem [GMW]: Such claims have ZK-proofs

I'll prove this claim in zero-knowledge

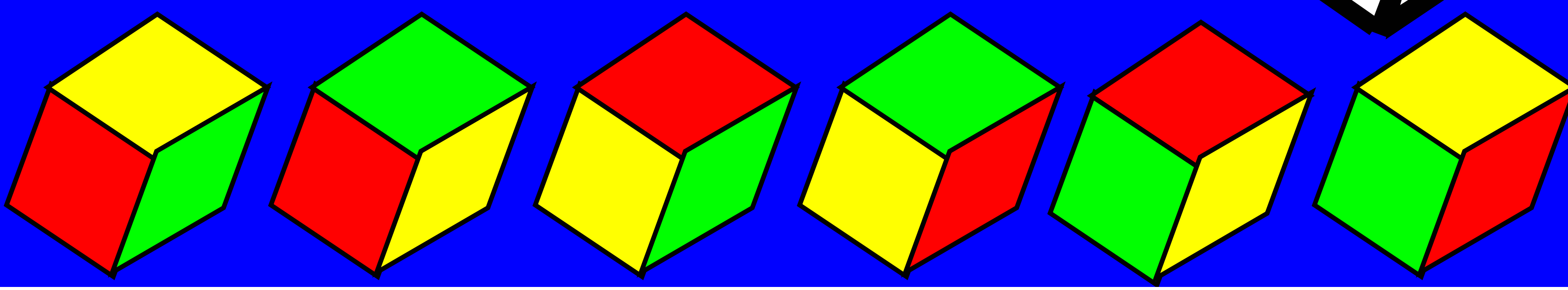
Claim: This map is 3-colorable (with R Y G)



Note: if I have any 3-coloring of any map



Then I immediately have 6



Structure of proof:

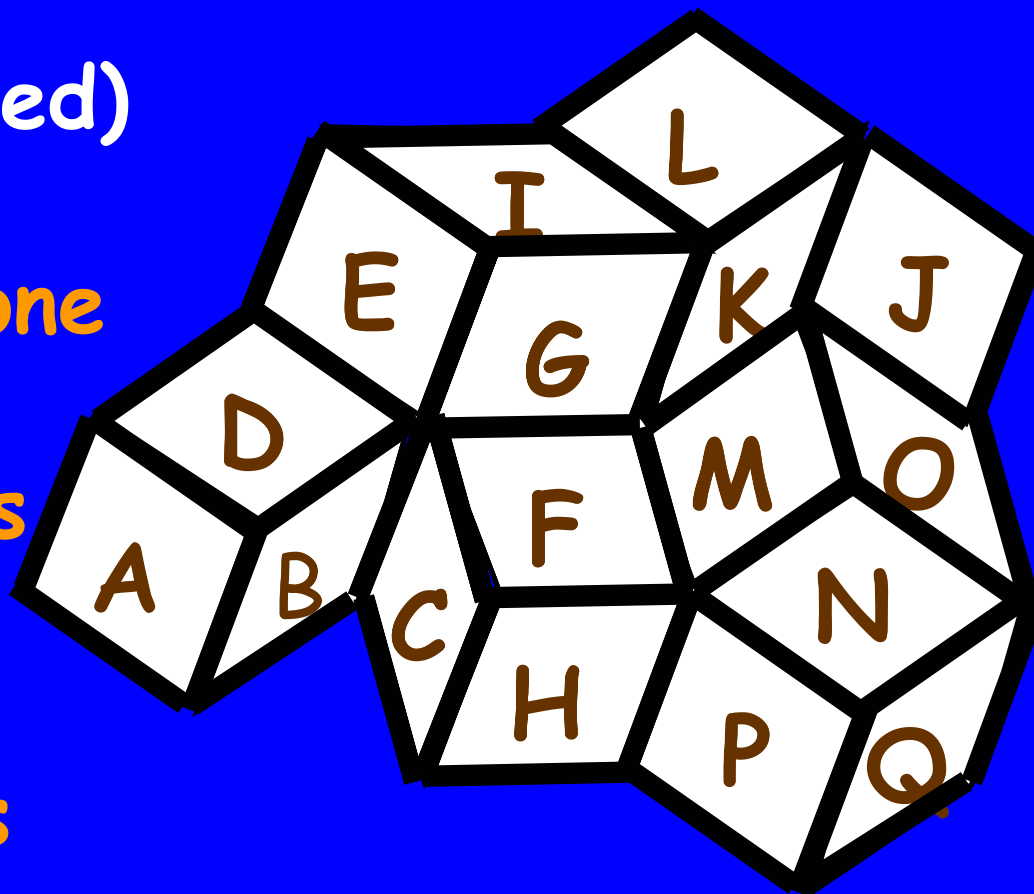
Repeat (until satisfied)

- I hide a random one of my 6 colorings in digital envelopes

- You pick a pair of adjacent countries

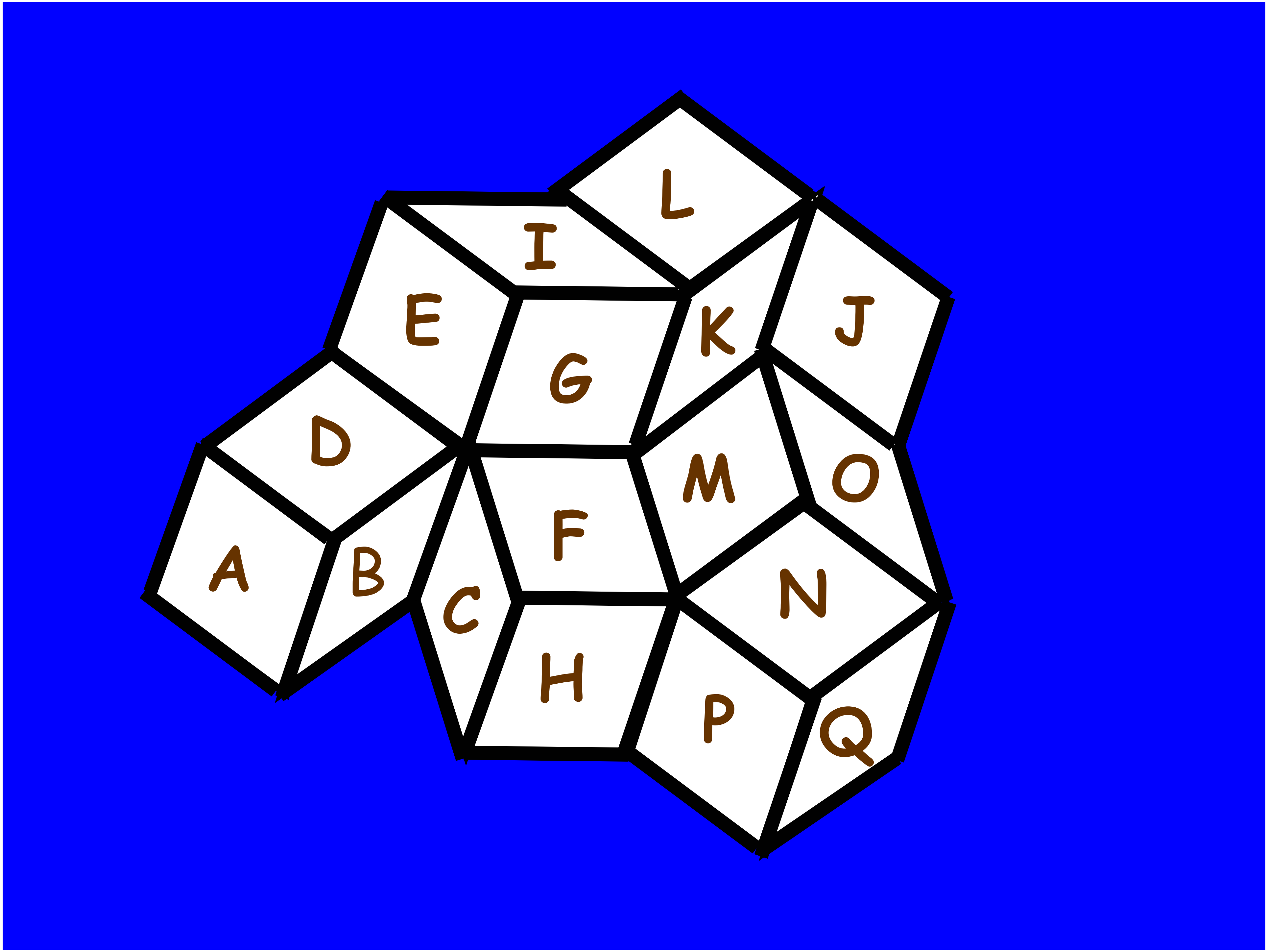
- I open this pair of envelopes

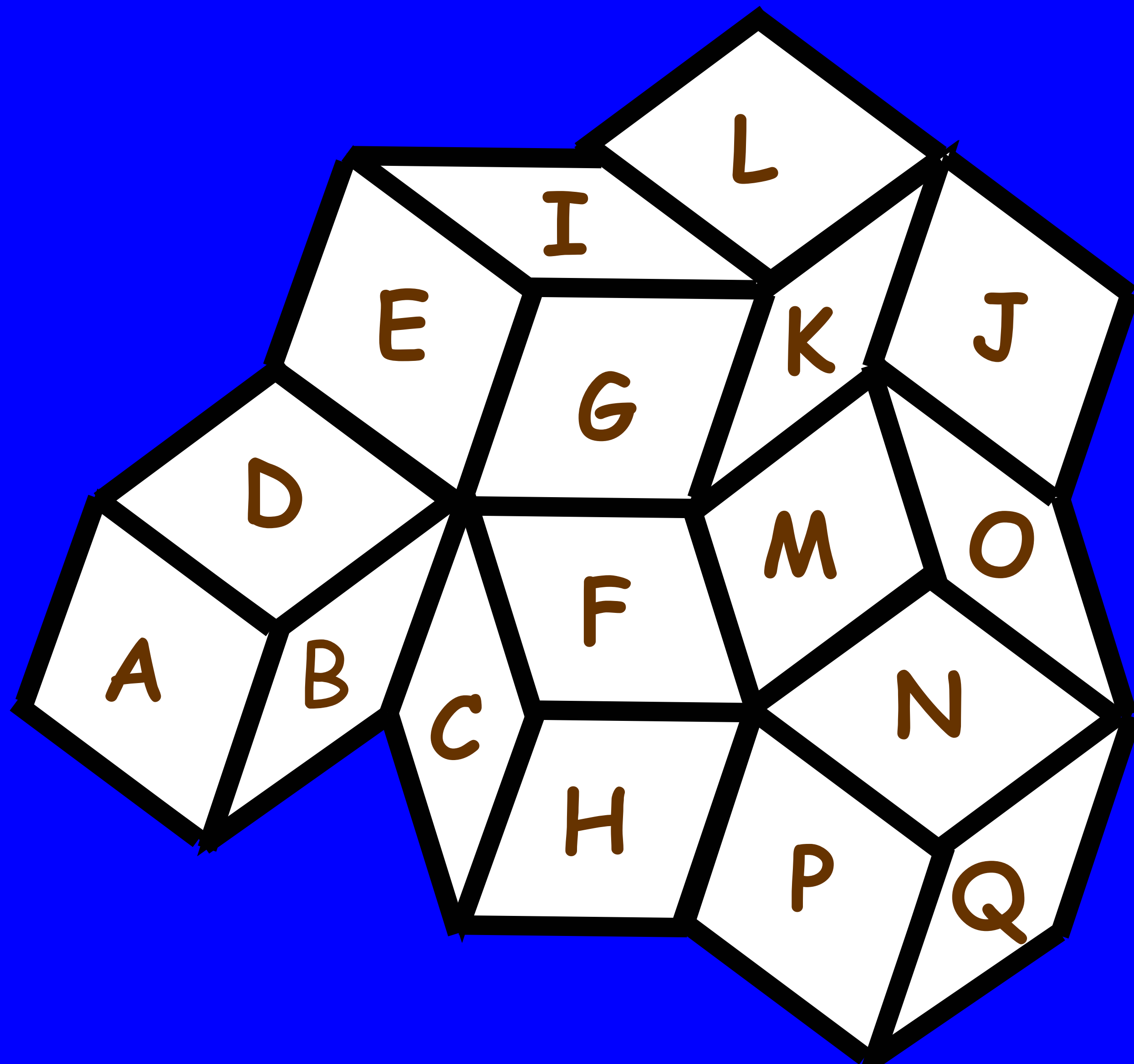
Reject if you see RR, YY, GG or illegal color

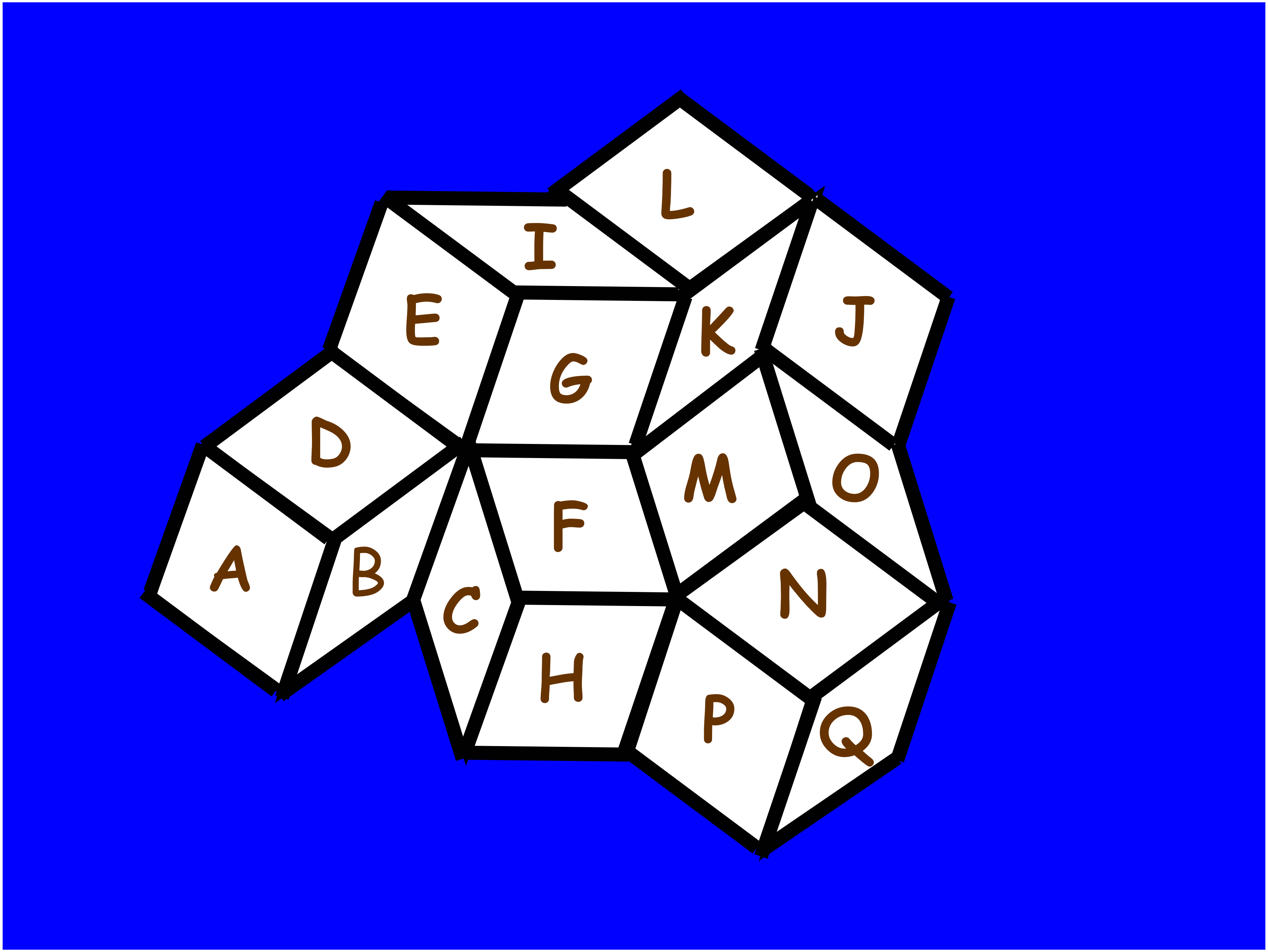


Zero-knowledge proof demo

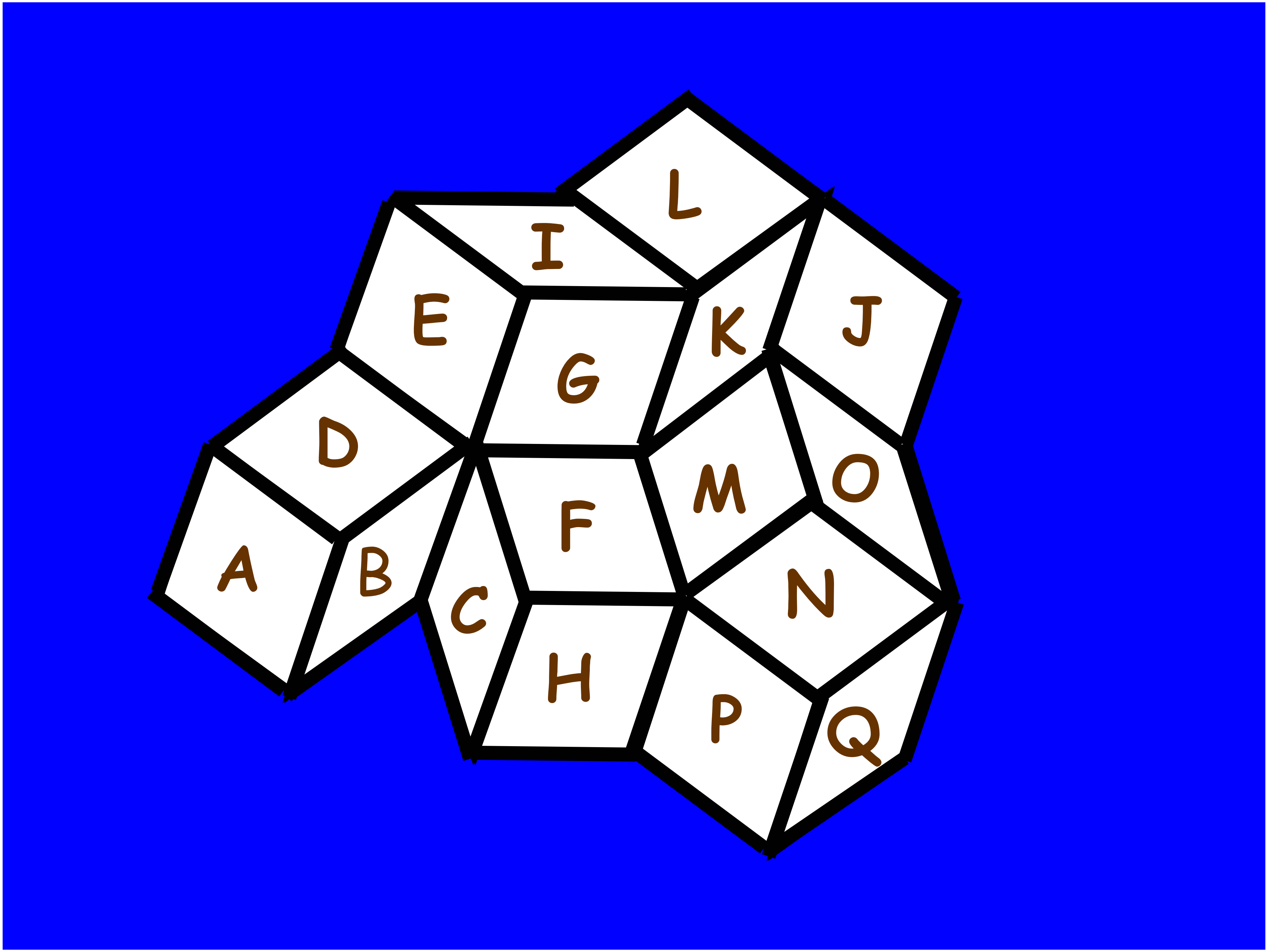
(open two adjacent envelopes on any subsequent slide)


L
I
E
G
K
J
D
M
O
F
A
B
C
N
H
P
Q

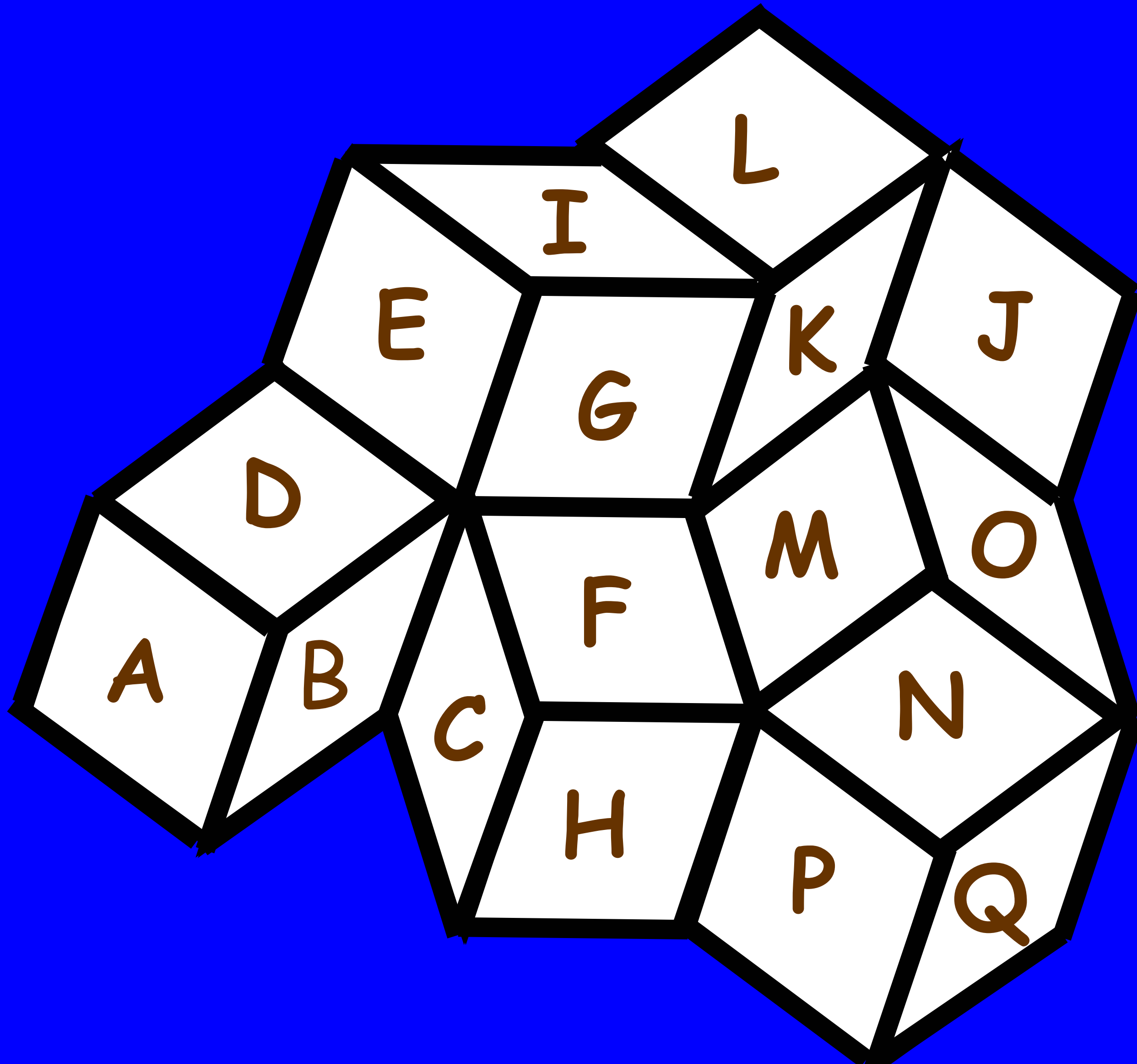

L
I
E
K
J
G
D
M
O
F
A
B
N
C
H
P
Q

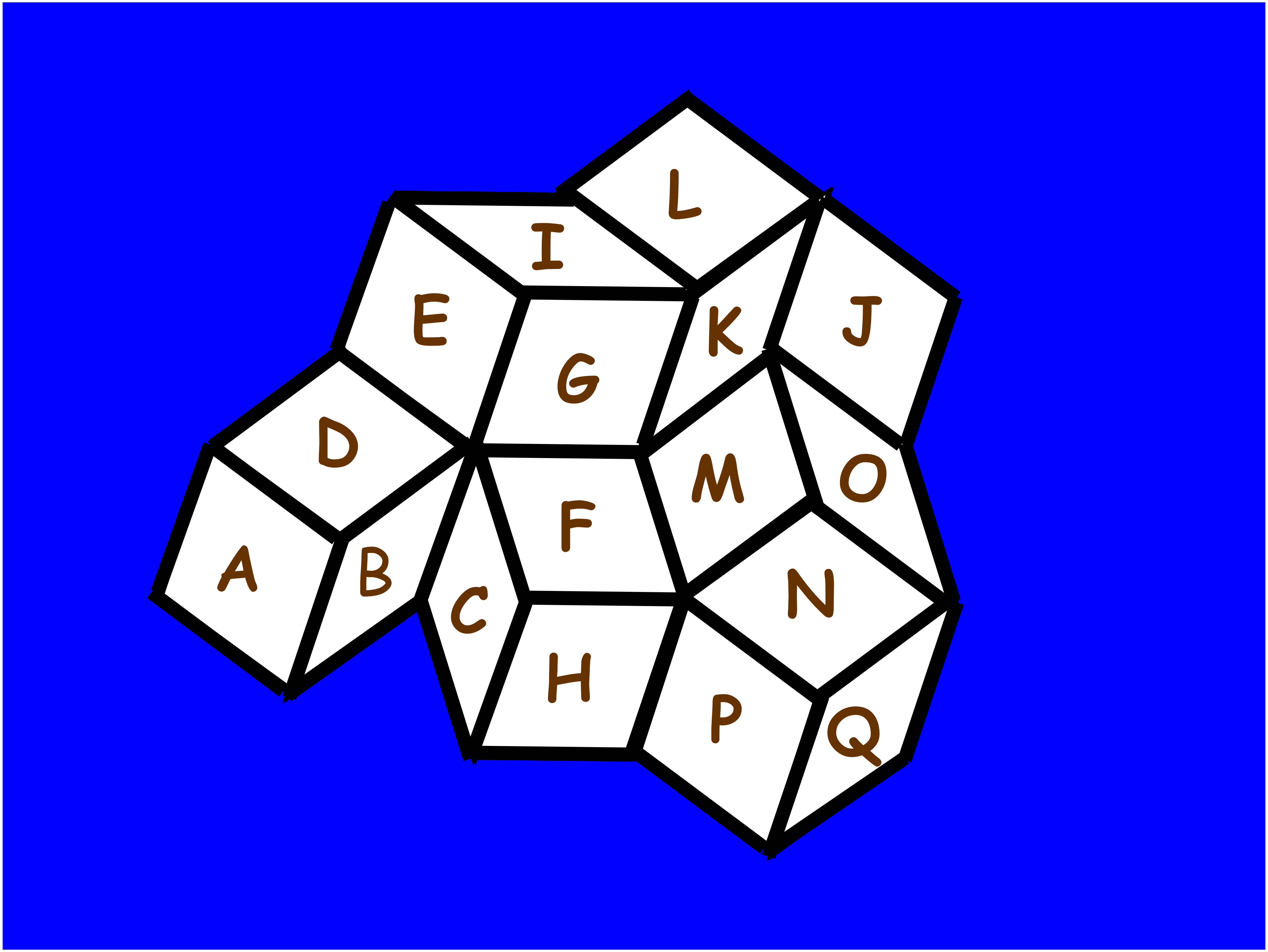


L
I
E
K
J
G
D
M
O
F
A
B
C
N
H
P
Q

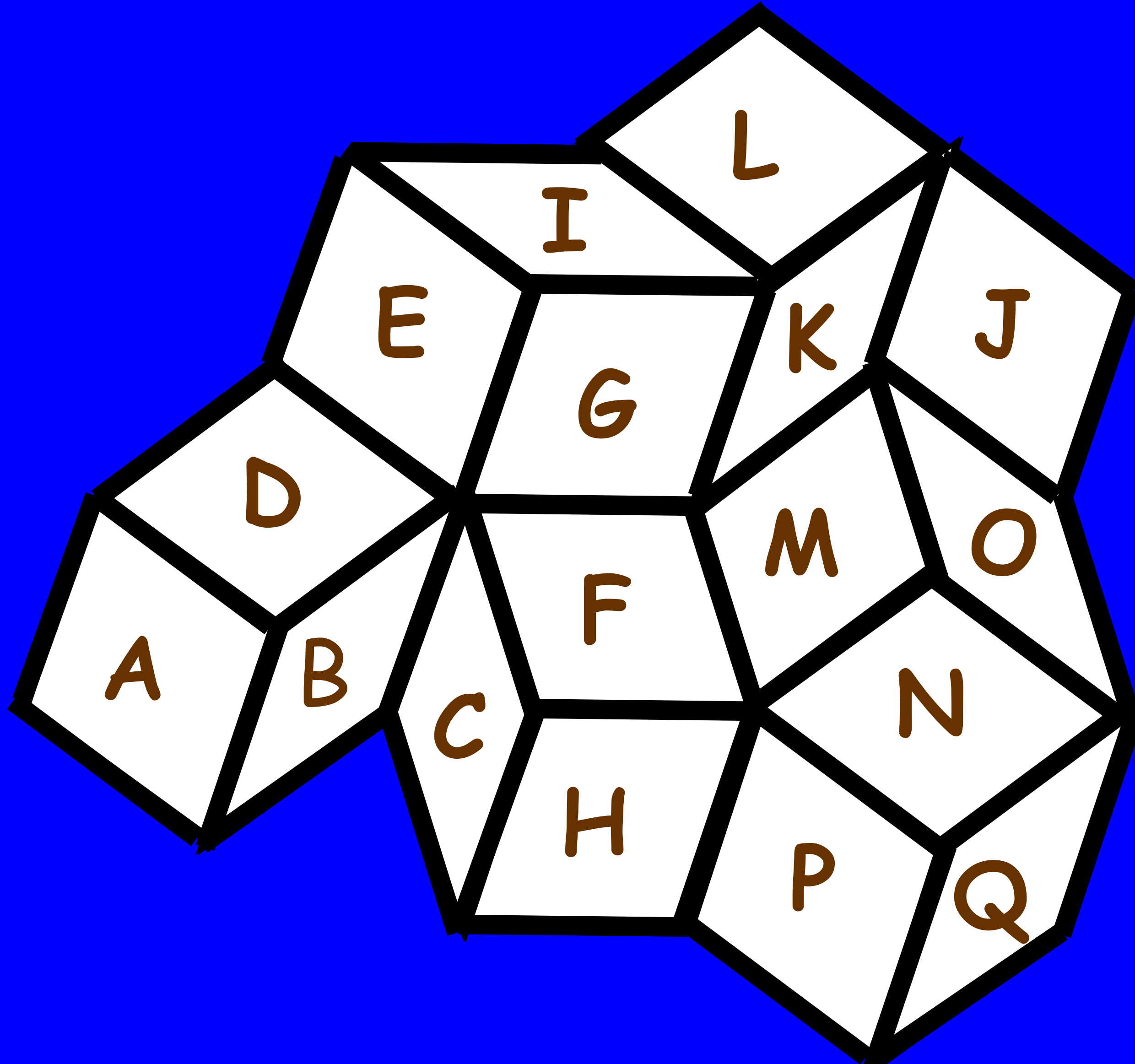


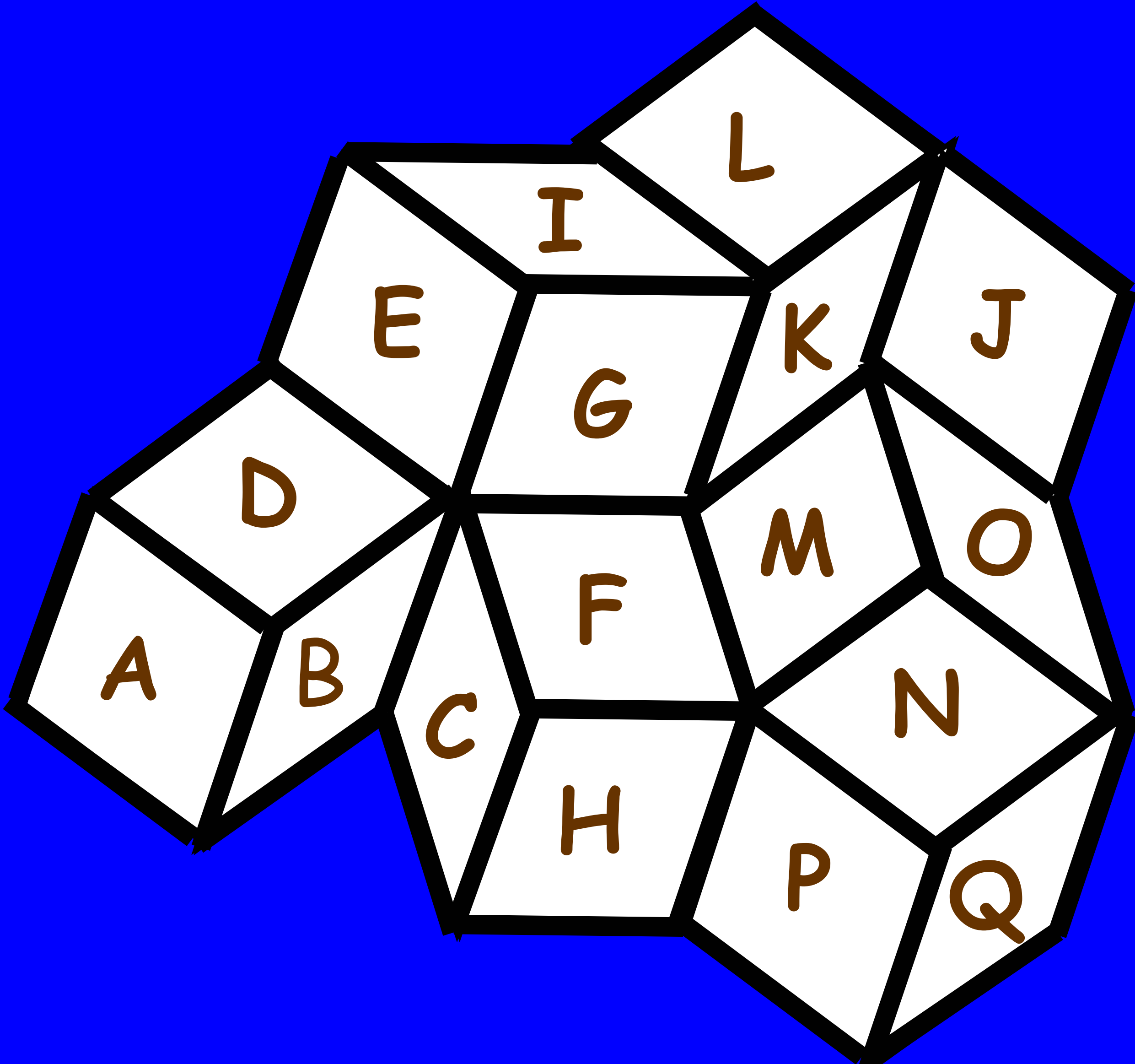
L
I
E
K
J
G
D
M
O
F
A
B
N
C
H
P
Q

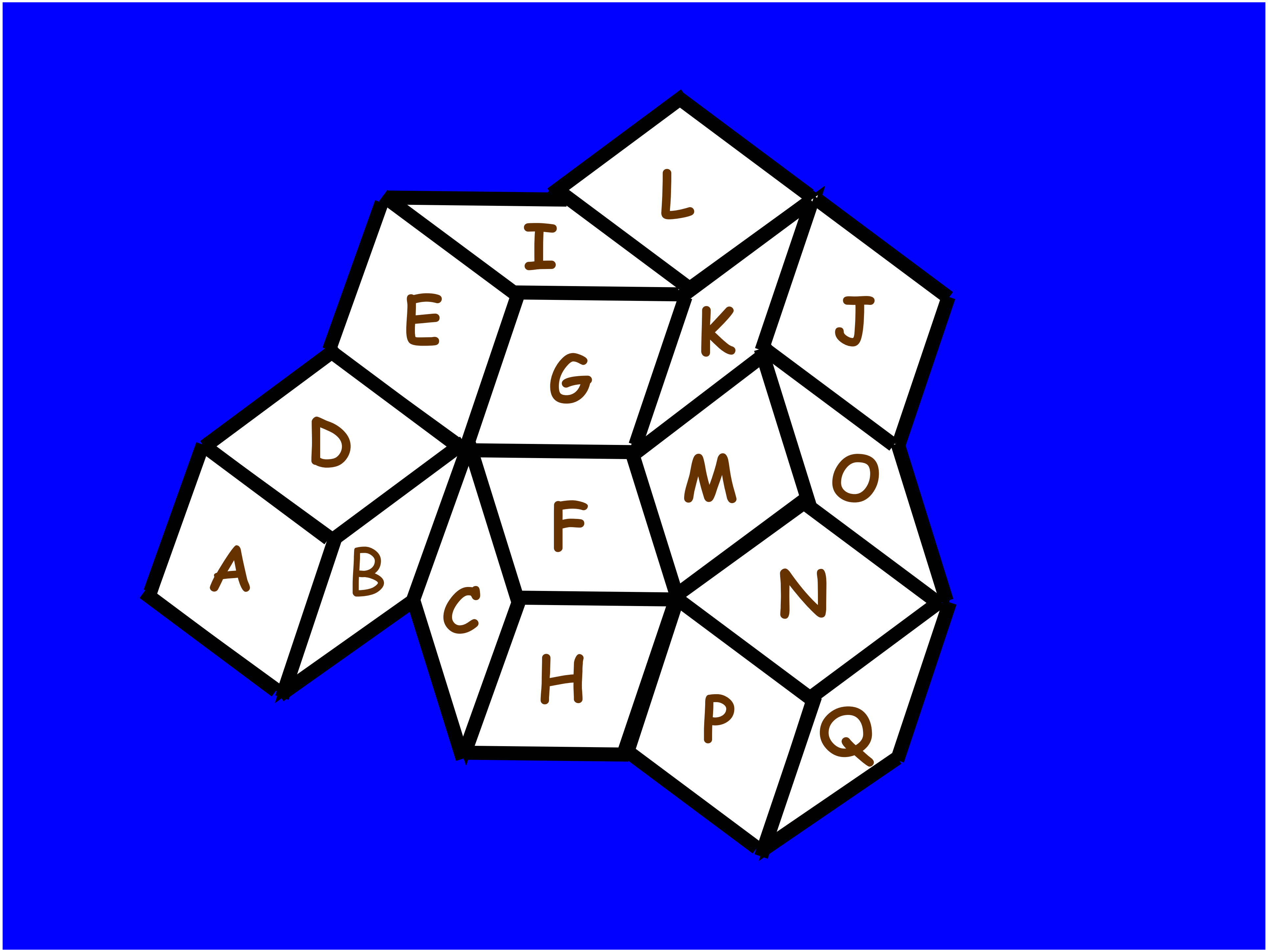

L
I
E
K
J
G
D
M
O
F
A
B
N
C
H
P
Q

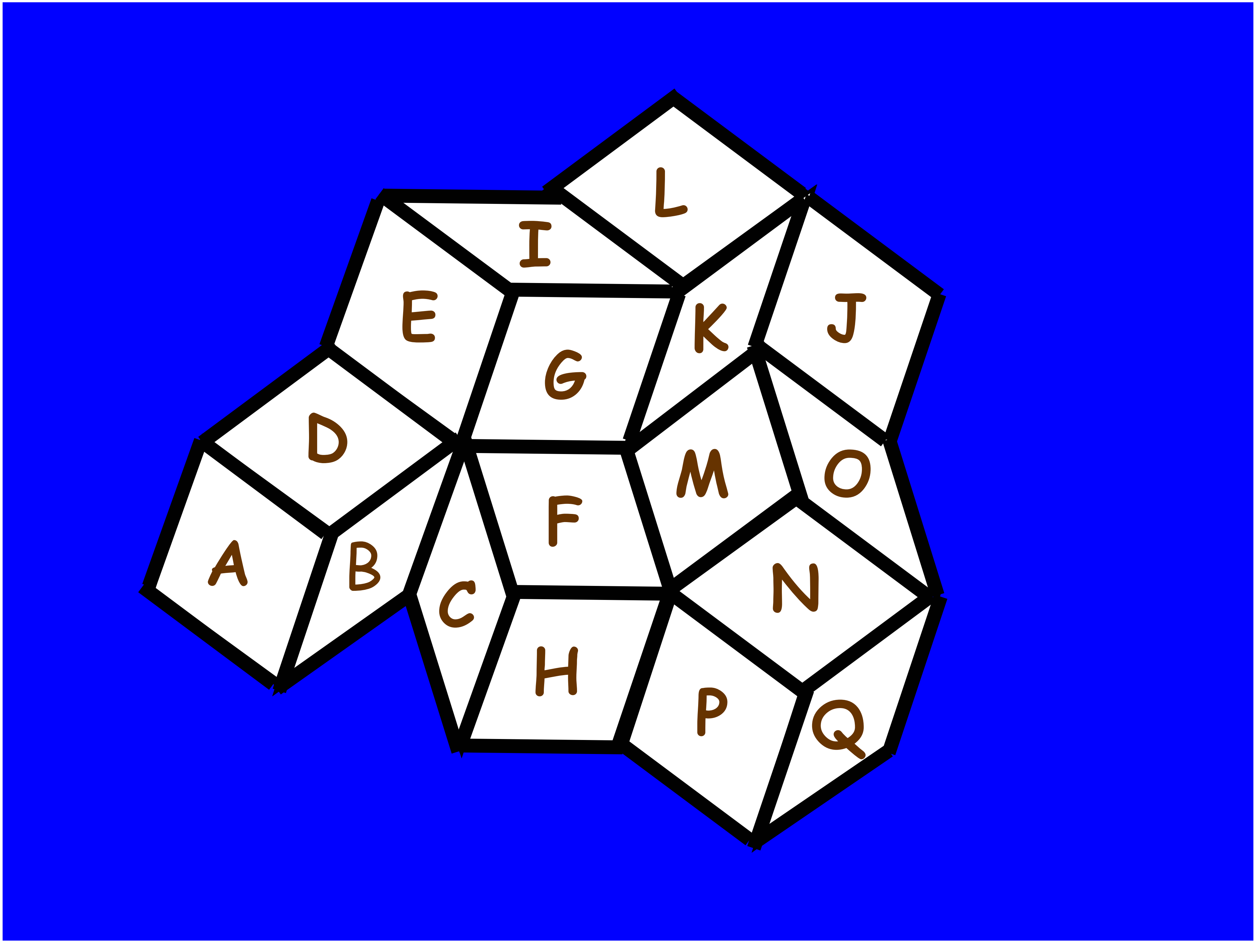


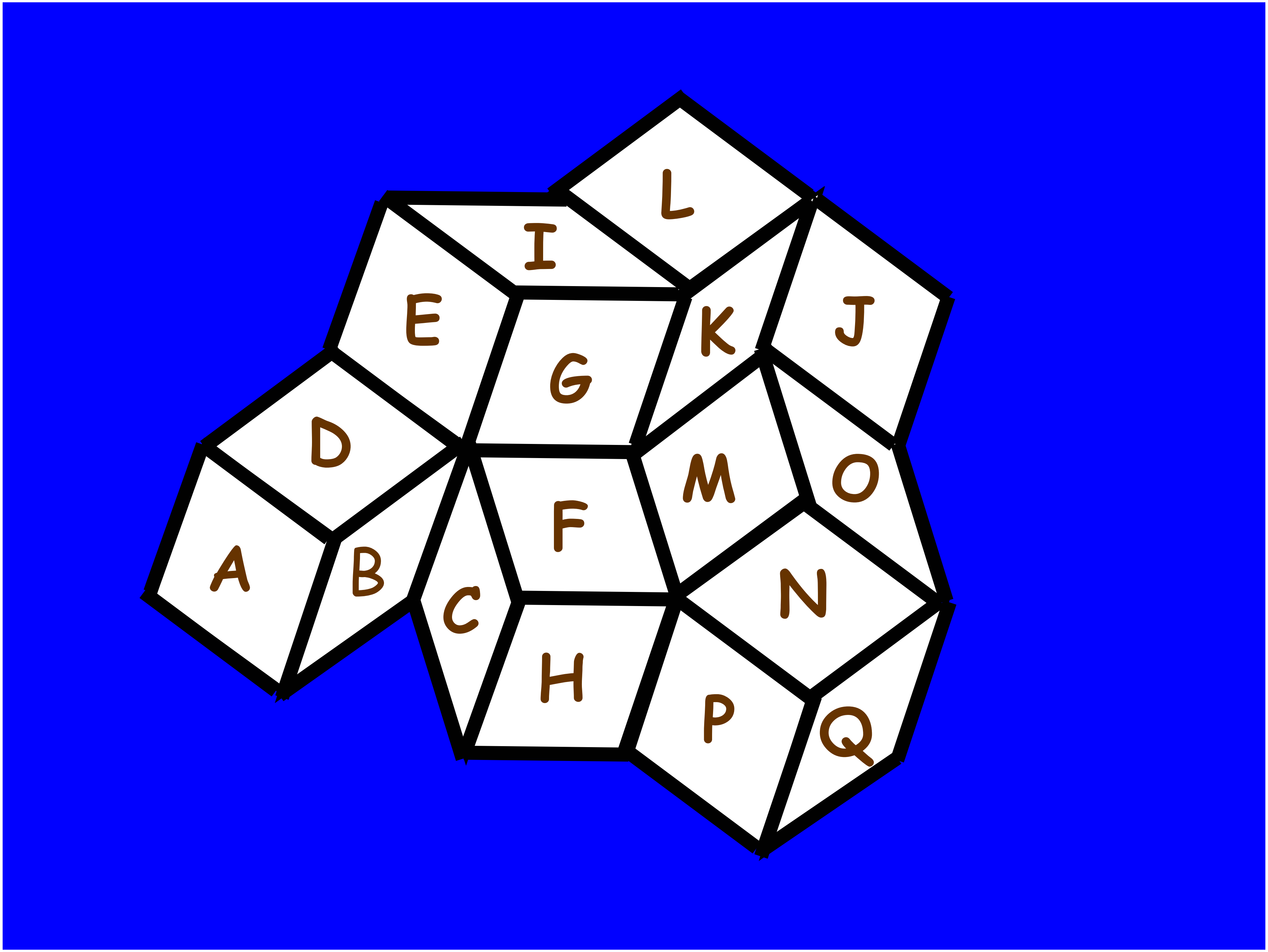
L
I
E
K
J
G
D
M
O
F
A
B
N
C
H
P
Q

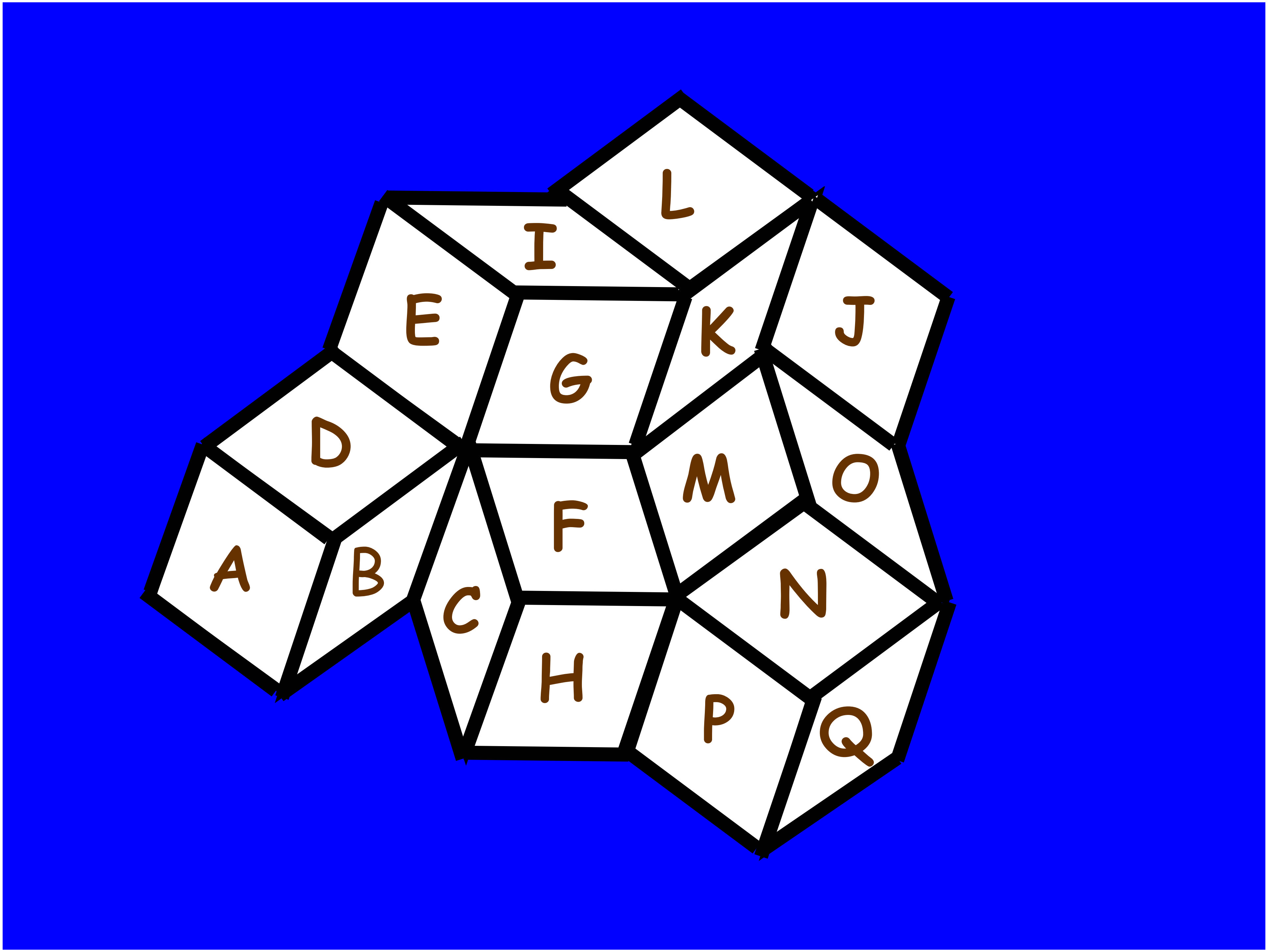

L
I
E
K
J
G
D
M
O
F
A
B
N
C
H
P
Q


L
I
E
K
J
G
D
M
O
F
A
B
C
N
H
P
Q


L
I
E
K
J
G
D
M
O
F
A
B
C
N
H
P
Q


L
I
J
E
K
G
D
M
O
F
A
B
N
C
H
P
Q


L
I
J
E
K
G
D
M
O
F
A
B
N
C
H
P
Q


L
I
J
E
K
G
D
M
O
F
A
B
N
C
H
P
Q

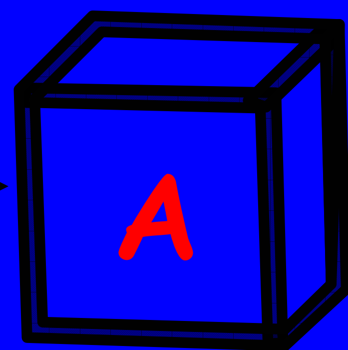
Why is it a Zero-Knowledge Proof?

- Exposed information is useless (random)
  Non-exposed info is useless (pseudorandom)
  (Bob learns nothing)*
- M 3-colorable $\rightarrow$ Probability [Accept] =1
  (Alice always convinces Bob)
- M not 3-colorable $\rightarrow$ Prob [Accept] < 1-1/n
  $\rightarrow$ Prob [Accept in n^2 trials] < exp(-n)
  (Alice rarely convince Bob)

[Formalizing this argument is quite complex!]

What does it have to do with Riemann's Hypothesis?

Theorem: There is an efficient algorithm A:

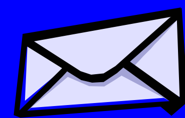
"Claim" +
"Proof length" → 

→ Map M

"Claim" true ⟷ M 3-colorable

"Proof" ⟶ 3-coloring of M

A is the Cook-Karp-Levin "dictionary",
Proving that 3-coloring is NP-complete

Theorem [GMW]:  + short proof
$\Rightarrow$ efficient ZK proof

$$\Downarrow$$

Theorem [GMW]:  $\Rightarrow$ fault-tolerant protocols

Summary

Practically every cryptographic task can be performed securely & privately

Assuming that players are computationally bounded, and that Factoring is hard.

- Computational complexity is essential!
- Randomness is essential for defining secrets
- Pseudorandomness essential for security proofs
- Hard problems can be useful!
- The theory predated (& enabled) the Internet

- What if factoring is easy? Few alternatives!

Open Q1: Base cryptography on proven hardness

Open Q2: Model physical attacks realistically