Mystery in Mathematics: Diffie-Hellman Key Exchange

Jim Fowler (@kisonecat)
Department of Mathematics
The Ohio State University

January 13, 2016

Mystery of Mathematics

Wigner, Eugene P. "The unreasonable effectiveness of mathematics in the natural sciences." *Communications on pure and applied mathematics* 13, no. 1 (1960): 1–14.

Putnam, Hilary. "What is mathematical truth?" *Historia Mathematica* 2, no. 4 (1975): 529–533.

Cheng, Eugenia. "Mathematics, morally." (2004).

Mathematics of Mystery

Can two friends, Alice and Bob, communicate in public (with eavesdroppers!) and nevertheless come to agree on a secret only they share?

Alice's Mind The Room Bob's Mind

Alice's Mind The Room Bob's Mind

"Start with ..."

Alice's Mind

The Room

Bob's Mind

Pick

"Start with ..."

Alice's Mind

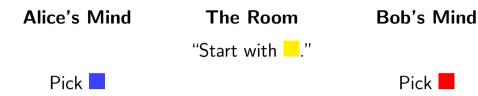
The Room

Bob's Mind

"Start with ..."

Pick





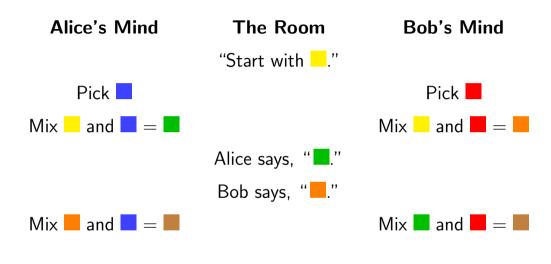
Mix and =

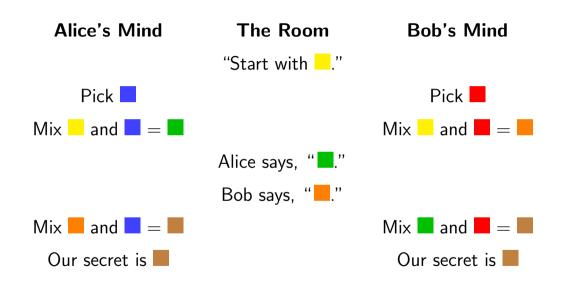












Alice's Mind The Room Bob's Mind

Alice's Mind The Room Bob's Mind

"Start with <mark>2</mark>."

Alice's Mind The Room

Bob's Mind

"Start with 2."

Pick 24.

Alice's Mind The Room

Pick 24.

"Start with 2."

Pick 17.

Bob's Mind

Alice's Mind

The Room

Bob's Mind

Pick 24.

"Start with 2."

Pick 17.

M(2, 24) = 20.

Alice's Mind

The Room
"Start with 2."

Bob's Mind

Pick 24.

Pick 17.

M(2, 24) = 20.

Alice says, "20."

Alice's Mind The Room

"Start with 2."

Pick 24.

M(2, 24) = 20.

Alice says, "20."

M(2, 17) = 21.

Bob's Mind

Pick 17.

Alice's Mind The Room Start with 2." Pick 24. Pick 17. M(2, 24) = 20. M(2, 17) = 21.

Alice says, "20."

Bob says, "21."

"Start with 2." Pick 24.

$$M(2, 24) = 20.$$

Alice's Mind

$$M(21, 24) = 25.$$

The Room

Bob's Mind

$$M(2, 17) = 21.$$

Alice's Mind The Room Boh's Mind "Start with 2." Pick 17. Pick 24. M(2, 24) = 20. M(2, 17) = 21. Alice says, "20." Bob says, "21." M(21, 24) = 25. M(20, 17) = 25.

Alice's Mind	The Room	Bob's Mind
	"Start with <mark>2</mark> ."	
Pick 24.		Pick 17.
M(2, 24) = 20.		M(2, 17) = 21.
	Alice says, " <mark>20</mark> ."	
	Bob says, " <mark>21</mark> ."	
M(21, 24) = 25.		M(20, 17) = 25.

Our secret is 25.

Our secret is 25.

Why does this work?

In this case,

$$M(M(2, 24), 17) = M(M(2, 17), 24).$$

Why does this work?

In this case,

In general,

$$M(M(2, 24), 17) = M(M(2, 17), 24).$$

M(M(2,a),b) = M(M(2,b),a).

Why does this work?

In this case,

$$M(M(2,24),17) = M(M(2,17),24).$$

In general,

$$M(M(2,a),b) = M(M(2,b),a).$$

Why does "Why does this work?" work?

Thank You

http://go.osu.edu/mystery

