

Mystery in Mathematics: Diffie-Hellman Key Exchange

Jim Fowler
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).

Mystery from Mathematics

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

“Start with .

Pick 

Alice's Mind

Pick 

The Room

“Start with .

Bob's Mind

Pick 

Alice's Mind

Pick 

Mix  and  = 

The Room

“Start with .

Bob's Mind

Pick 

Alice's Mind

Pick 

Mix  and  = 

The Room

“Start with .

Alice says, “.

Bob's Mind

Pick 


Alice's Mind

Pick 

Mix  and  = 

The Room

"Start with .

Alice says, ".

Bob's Mind

Pick 

Mix  and  = 


Alice's Mind


Pick 

Mix  and  = 

The Room

"Start with .

Alice says, ".

Bob says, ".

Bob's Mind

Pick 

Mix  and  = 

Alice's Mind


Pick 

Mix  and  = 

Mix  and  = 

The Room

"Start with .

Alice says, ".

Bob says, ".

Bob's Mind

Pick 

Mix  and  = 

Alice's Mind


Pick 


Mix  and  = 

Mix  and  = 

The Room

"Start with .

Alice says, ".

Bob says, ".

Bob's Mind

Pick 

Mix  and  = 

Mix  and  = 

Alice's Mind

Pick 

Mix  and  = 

Mix  and  = 

Our secret is 

The Room

"Start with .

Alice says, ".

Bob says, ".

Bob's Mind

Pick 

Mix  and  = 

Mix  and  = 

Our secret is 

Alice's Mind

The Room

Bob's Mind

Alice's Mind

The Room

Bob's Mind

“Start with 2.”

Alice's Mind

Pick 24.

The Room

“Start with 2.”

Bob's Mind

Alice's Mind

Pick **24**.

The Room

“Start with **2**.”

Bob's Mind

Pick **17**.

Alice's Mind

Pick 24.

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

The Room

"Start with 2."

Bob's Mind

Pick 17.

Alice's Mind

Pick 24.

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

The Room

"Start with 2."

Alice says, "20."

Bob's Mind

Pick 17.

Alice's Mind

Pick 24.

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

The Room

"Start with 2."

Alice says, "20."

Bob's Mind

Pick 17.

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

Alice's Mind

Pick 24.

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

The Room

"Start with 2."

Alice says, "20."

Bob says, "21."

Bob's Mind

Pick 17.

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

Alice's Mind

Pick 24.

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

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

The Room

"Start with 2."

Alice says, "20."

Bob says, "21."

Bob's Mind

Pick 17.

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

Alice's Mind

Pick 24.

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

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

The Room

"Start with 2."

Alice says, "20."

Bob says, "21."

Bob's Mind

Pick 17.

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

$$M(20, 17) = 25.$$

Alice's Mind

Pick 24.

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

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

Our secret is 25.

The Room

"Start with 2."

Alice says, "20."

Bob says, "21."

Bob's Mind

Pick 17.

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

$$M(20, 17) = 25.$$

Our secret is 25.

Why does this work?

In this case,

$$M(M(\text{2}, \text{24}), \text{17}) = M(M(\text{2}, \text{17}), \text{24}).$$

In general,

$$M(M(\text{2}, a), b) = M(M(\text{2}, b), a).$$

Thank You

