Diffie-Hellman Key Exchange

Dr Rosanne English

Diffie-Hellman Key Exchange (DHKE)

- Allows a private symmetric key to be established over an insecure channel in such a way that an attacker cannot derive the key from the messages sent.
- Provides a solution to the key exchange problem
- Variants of DHKE are used in end-to-end encrypted messaging platforms such as Whatsapp and Signal

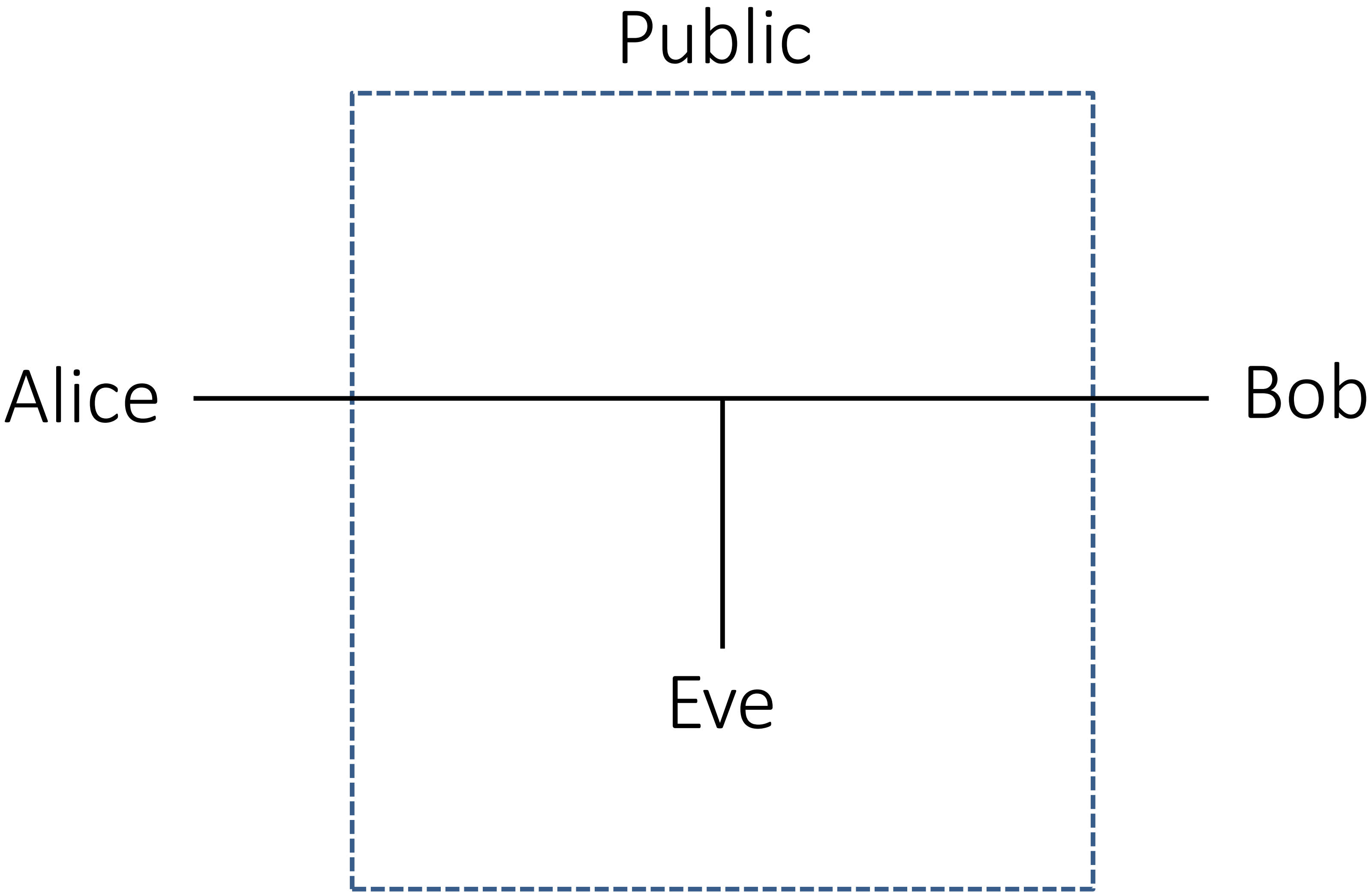
Mathematical concepts in DHKE

modular arithmetic is where we are only interested in the remainder upon division by an integer. Given two integers A and B, A/B = Q mod R where Q is the quotient (the number of times B completely divides A) and R is the remainder. For example, 15 mod 12 is congruent to 3.

g is a primitive root modulo *n* if and only if every integer *a which is* coprime with *n* is congruent to a power of *g* mod *n*

$g^k \equiv a \ (mod\ n)$ where k is a positive integer

Communication Network



Public

Alice

Bob

Eve

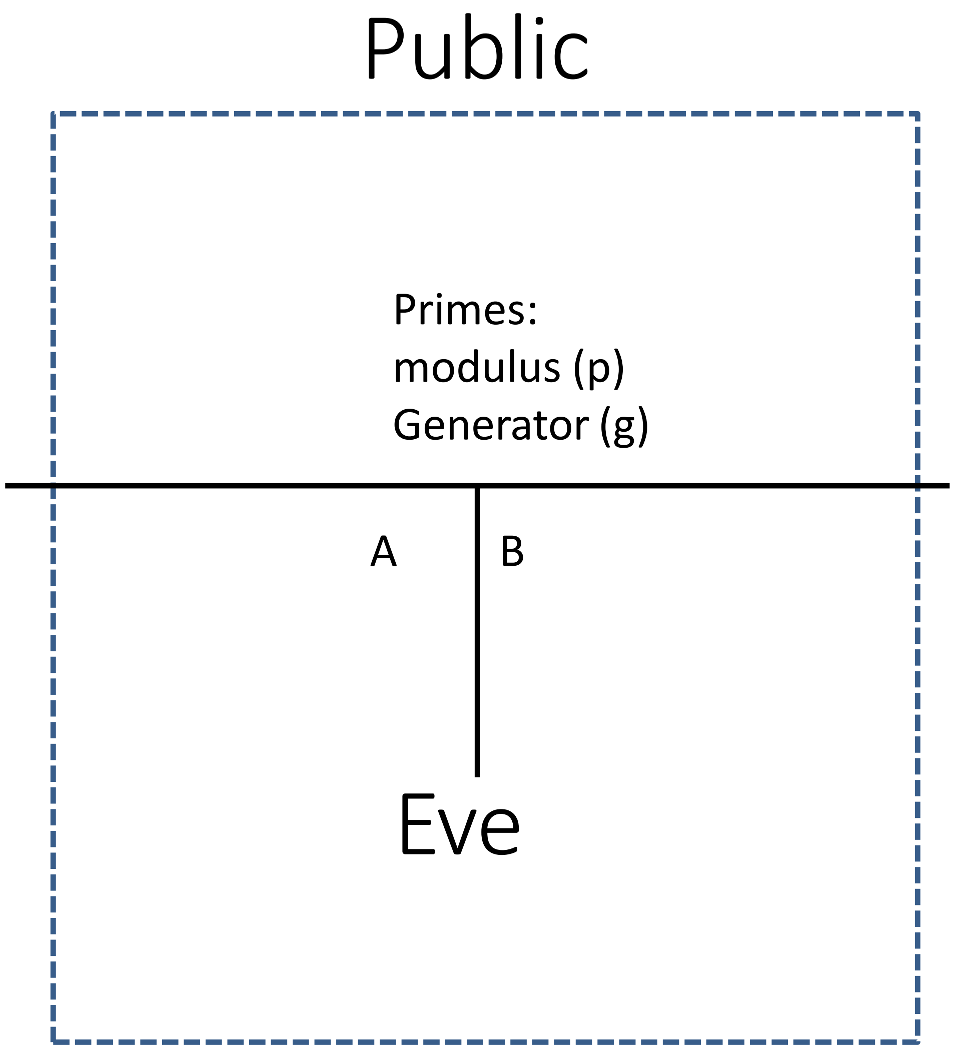
Diffie-Hellman Key Exchange

Alice

Selects private random number a

Calculates:
A= g^a mod p

Calculates:
K = B^amod p



Public

Primes:
modulus (p)
Generator (g)

A

B

Eve

Bob

Selects a private random number b

Calculates:
B=g^b mod p

Calculates:
K = A^b mod p