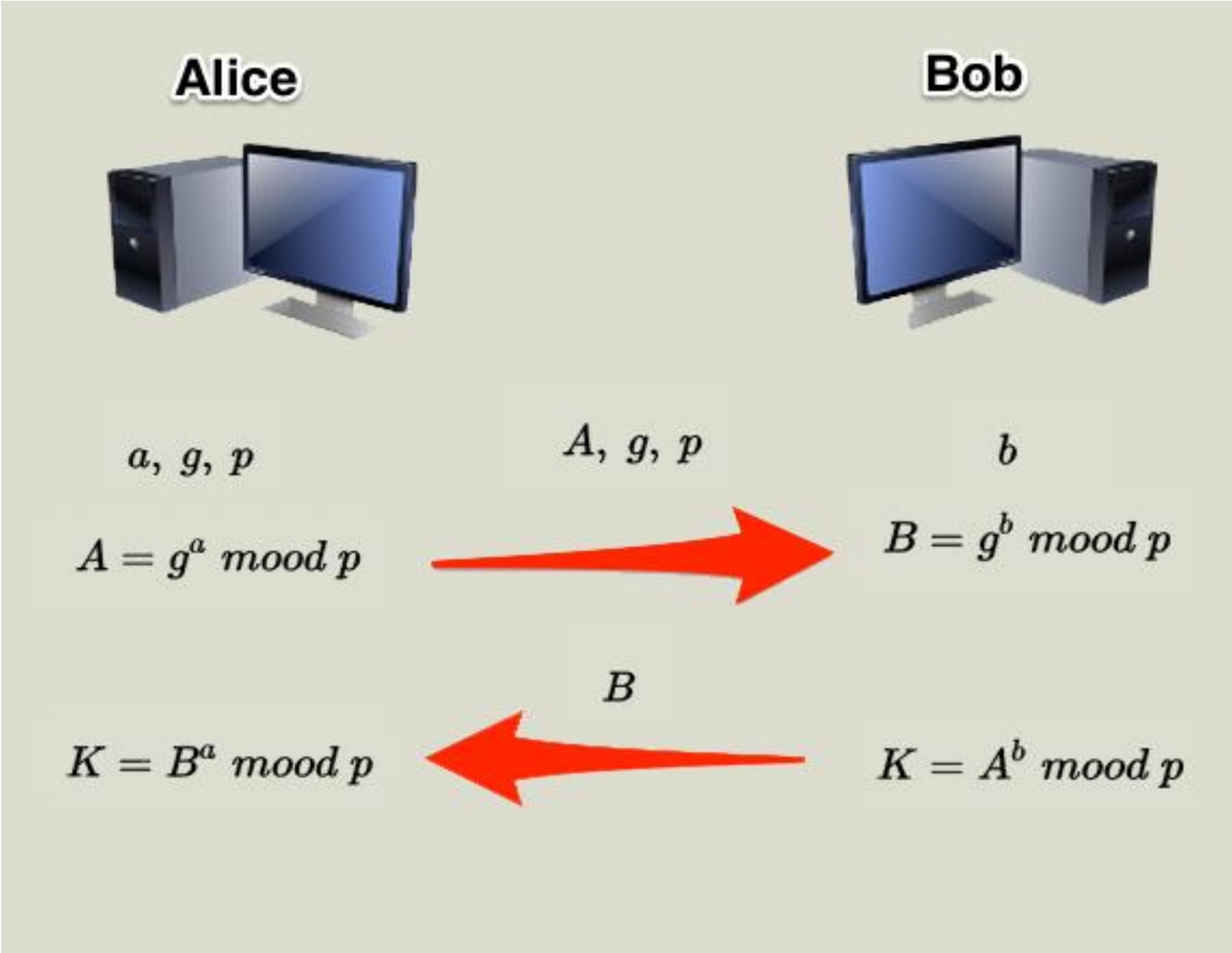
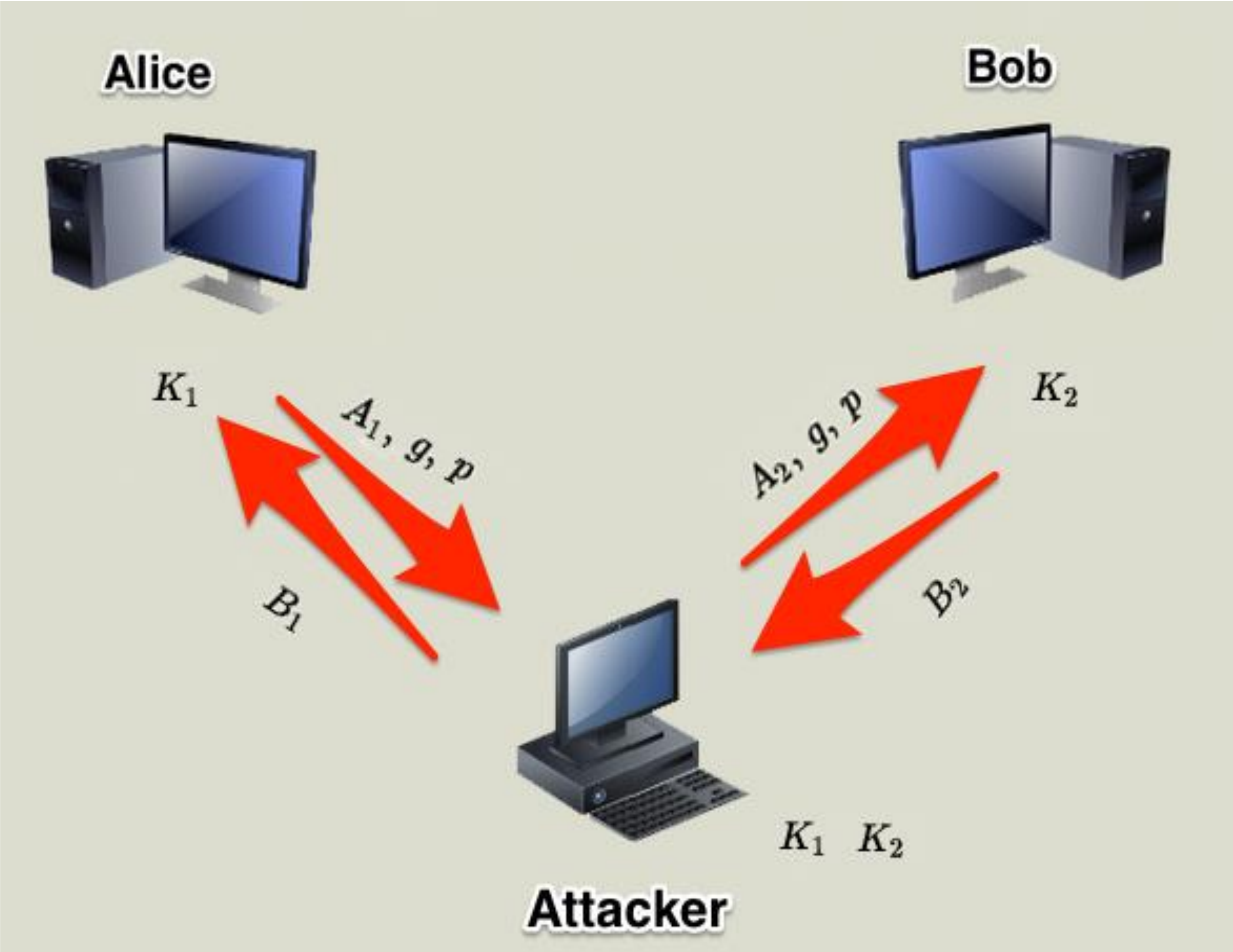

Alice
Bob
$a,\ g,\ p$
$A,\ g,\ p$
b
$A = g^a$ mood p
$B = g^b$ mood p
B
$K = B^a$ mood p
$K = A^b$ mood p


Alice
Bob
K_1
K_2
A_1, g, p
B_1
A_2, g, p
B_2
K_1 K_2
Attacker

- In modular arithmetic, a branch of number theory, a number g is a **primitive root modulo n** if every number a coprime to n is congruent to a power of g modulo n. That is, for every integer a coprime to n, there is an integer k such that $g^k \equiv a \pmod{n}$. Such k is called the **index** or **discrete logarithm** of a to the base g modulo n.

- In other words, g is a generator of the multiplicative group of integers modulo n.

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms. Briefly, we can define the discrete logarithm in the following way. Recall from Chapter 8 that a primitive root of a prime number p as one whose powers modulo p generate all the integers from 1 to $p - 1$. That is, if a is a primitive root of the prime number p, then the numbers

$$a \bmod p,\ a^2 \bmod p,\ \ldots,\ a^{p-1} \bmod p$$

are distinct and consist of the integers from 1 through $p - 1$ in some permutation.

For any integer b and a primitive root a of prime number p, we can find a unique exponent i such that

$$b \equiv a^i \pmod{p} \qquad \text{where } 0 \leq i \leq (p - 1)$$

The exponent i is referred to as the **discrete logarithm** of b for the base a, mod p. We express this value as $\mathrm{dlog}_{a,p}(b)$. See Chapter 8 for an extended discussion of discrete logarithms.

Asymmetric Encryption: RSA

- Choose two large prime numbers p & q
- Compute $n=pq$ and $z=(p-1)(q-1)$
- Choose number e, less than n, which has no common factor (other than 1) with z
- Find number d, such that $ed – 1$ is exactly divisible by z
- Keys are generated using n, d, e
  - Public key is (n,e)
  - Private key is (n, d)
- Encryption: $c = m^e \bmod n$
  - m is plain text
  - c is cipher text
- Decryption: $m = c^d \bmod n$
- Public key is shared and the private key is hidden

Asymmetric Encryption: RSA

- P=5 & q=7
- n=5*7=35 and z=(4)*(6) = 24
- e = 5
- d = 29 , (29x5 = 1 mod 24)
- Keys generated are
  - Public key: (5, 35)
  - Private key is (29, 35)
- Encrypt the word love using ($c = m^e \bmod n$)
  - Assume that the alphabets are between 1 & 26

Plain Text	Numeric Representation	m^e	Cipher Text ($c = m^e \bmod n$)
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

Asymmetric Encryption: RSA

- Decrypt the word love using $(m = c^d \bmod n)$
  - d=29, n=35

Cipher Text	c^d	$(m = c^d \bmod n)$	**Plain Text**
17	481968572106750915091411825223072000	12	l
15	127834039488589391112327575683594000	15	o
22	852643319086537701956194499721110000000	22	v
10	100000000000000000000000000000	5	e