Host A   Router A   Router B   Host B

1. Host A sends interesting traffic to Host B.
2. Routers A and B negotiate an IKE phase one session.

IKE SA ← IKE Phase 1 → IKE SA

3. Routers A and B negotiate an IKE phase two session.

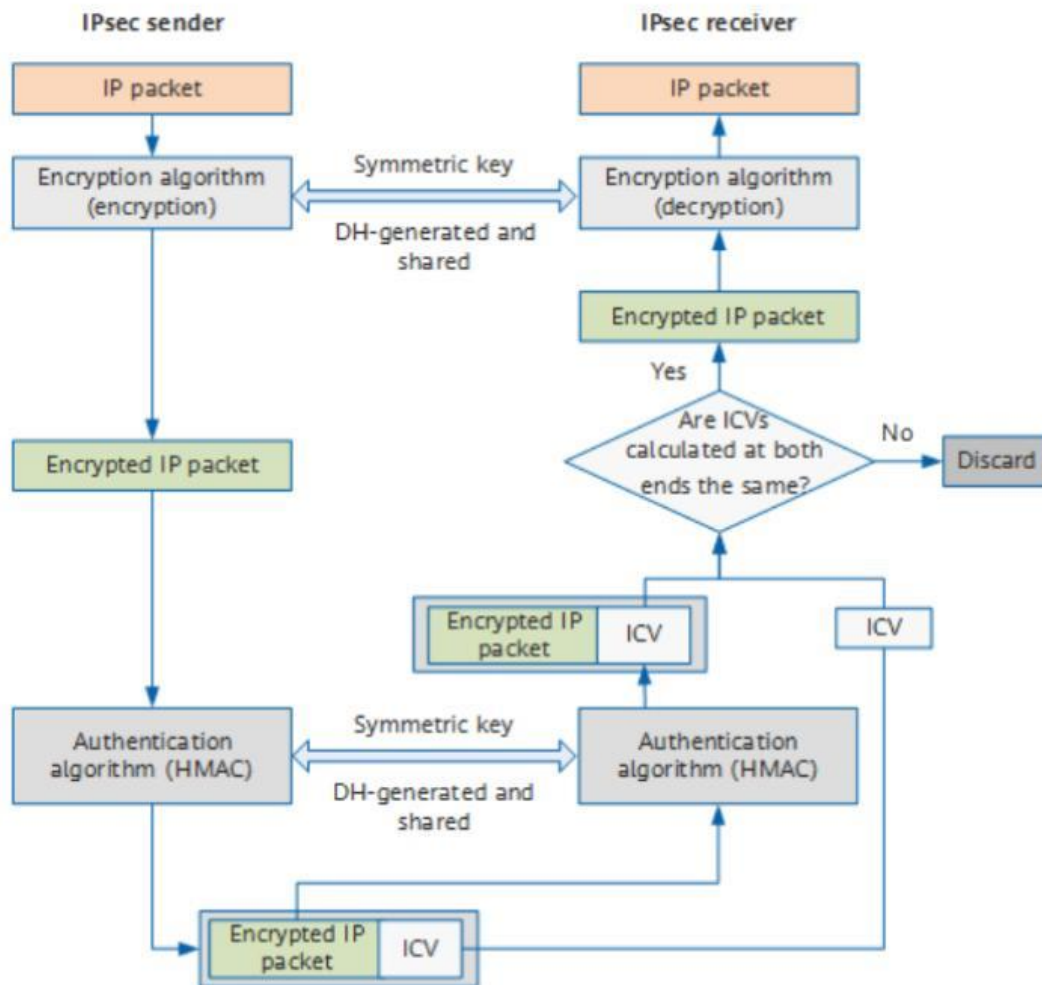IPSec SA ← IKE Phase 2 → IPSec SA
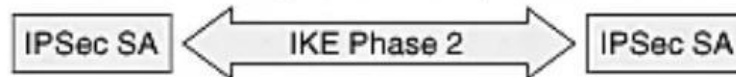
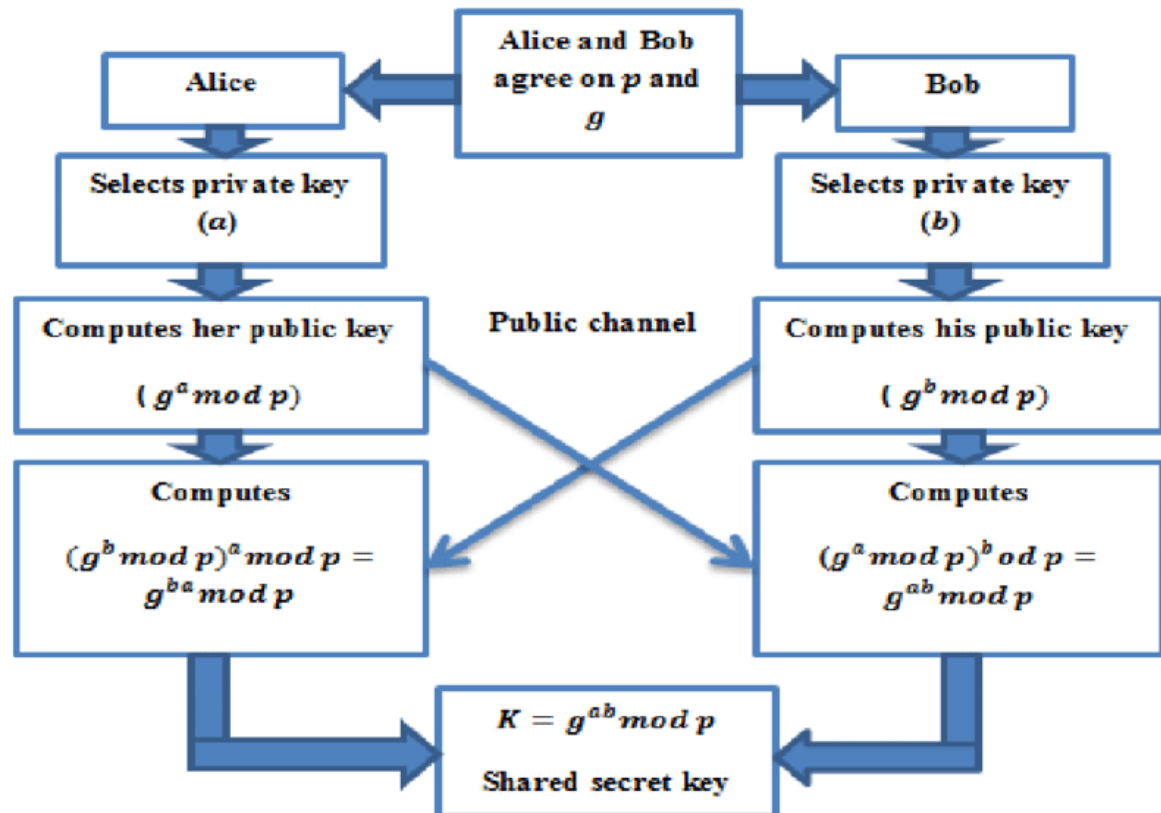4. Information is exchanged via IPSec tunnel.

←   IPSec Tunnel   →

5. IPSec tunnel is terminated.

Step 4 (In detail):

IPsec encryption and authentication process

Step 2 (DH Key exchange In detail)

```
                    ┌─────────────────┐
┌──────────┐        │  Alice and Bob  │        ┌──────────┐
│  Alice   │◄───────│ agree on p and  │───────►│   Bob    │
└──────────┘        │        g        │        └──────────┘
     │              └─────────────────┘             │
     ▼                                               ▼
┌──────────────────┐                      ┌──────────────────┐
│ Selects private  │                      │ Selects private  │
│   key (a)        │                      │   key (b)        │
└──────────────────┘                      └──────────────────┘
     │                                               │
     ▼                                               ▼
┌──────────────────┐    Public channel    ┌──────────────────┐
│ Computes her     │                      │ Computes his     │
│ public key       │                      │ public key       │
│ (gᵃ mod p)       │                      │ (gᵇ mod p)       │
└──────────────────┘                      └──────────────────┘
     │                                               │
     ▼                                               ▼
┌──────────────────┐                      ┌──────────────────┐
│ Computes         │                      │ Computes         │
│ (gᵇ mod p)ᵃ      │                      │ (gᵃ mod p)ᵇ od p │
│ mod p = gᵇᵃ mod p│                      │ = gᵃᵇ mod p      │
└──────────────────┘                      └──────────────────┘
     │          ┌──────────────────┐               │
     └─────────►│ K = gᵃᵇ mod p    │◄──────────────┘
                │ Shared secret key│
                └──────────────────┘
```

Alice and Bob agree on p and g

Alice

Bob

Selects private key (a)

Selects private key (b)

Computes her public key $(g^a \bmod p)$

Public channel

Computes his public key $(g^b \bmod p)$

Computes $(g^b \bmod p)^a \bmod p = g^{ba} \bmod p$

Computes $(g^a \bmod p)^b od\, p = g^{ab} \bmod p$

$K = g^{ab} \bmod p$

Shared secret key

Example DH Key exchange:

Agree upon two numbers:

P	Prime Number	13
G	Generator of P	6

Randomly generate a Private Key

Private = 5

Private = 4

Calculate Public Key:

$(G^{Private})$ MOD P

(6^5) MOD 13
(7776) MOD 13
Public = 2

(6^4) MOD 13
(1296) MOD 13
Public = 9

Exchange Public Keys

Calculate the Shared Secret

$(Shared\ Public^{Private})$ MOD P

(9^5) MOD 13
(59049) MOD 13
Shared Secret = 3

(2^4) MOD 13
(16) MOD 13
Shared Secret = 3

PRACTICAL NETWORKING .NET