Diffie Hellman

Piotr Karamon

<2022-06-27 Mon>

1 Actual content

1.1 Alice/Bob example

a Alice's secret

b Bob's secret

n is a huge prime number

g is a constant (does not have to be big typically 2 or 5, which is a primitive root modulo n)

1.2 Steps of key exchange:

1. Alice computes $g^a \bmod n$
2. Bob computes $g^b \bmod n$
3. Alice sends g^a to Bob and Bob gives g^b to Alice
4. Alice computes $(g^b)^a \bmod n$ and Bob computes $(g^a)^b \bmod n$
5. The shared secret is the $g^{ab} \bmod n$

1.3 Python program showing more details

```python
n = 23
g = 5
a = 4
alice = {"a": 4}
bob = {"b": 3}

# first step
ga = (g**alice["a"]) % n # generated by Alice, sent to Bob
gb = (g**bob["b"]) % n # generated by Bob, sent to Alice
# ga, gb, g, n are public (meaning anyone who can intercept network can read them )

alice["gab"] = (gb ** alice["a"]) % n
bob["gab"] = (ga ** bob["b"]) % n

print("alice", alice["gab"]) # alice 18
print("bob", bob["gab"]) # bob 18
```

Results

```
alice 18
bob 18
```