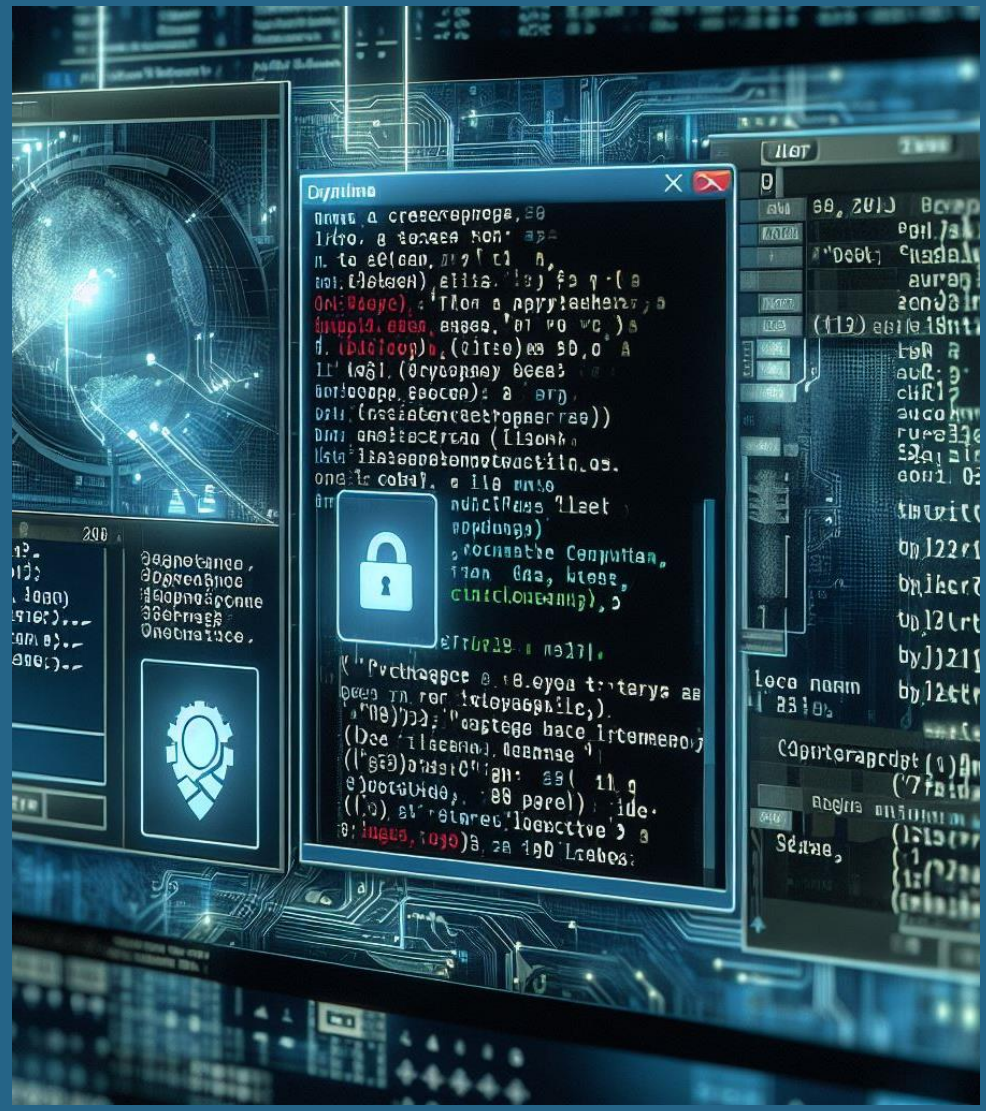
Public Key Cryptosystems
RSA

Horvath Krisztina-Aliz

Contents



What is a public-key cryptosystem?

- A public-key cryptosystem is a cryptographic method that uses a pair of mathematically linked keys – a public-key, freely shared, and a private key, kept secret.
- The public-key encrypts messages, and only the corresponding private key can decrypt them.

What is RSA?

- RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem, one of the oldest that is widely used for secure data transmission. Its security is based on the challenge of factoring large primes.

RSA Key Generation

1. Generates 2 random large distinct primes p, q of approximately same size.

2. Computes

$n = p * q$ and

$\varphi(n) = (p - 1)(q - 1)$ (the Euler function)

3. Randomly selects

$1 < e < \varphi(n)$ with

$\gcd(e, \varphi(n)) = 1$.

4. Computes

$d = e^{-1} \bmod \varphi(n)$.

5. Bob's public key is

$K_E = (n, e)$; his private key is

$K_D = d$.

Encryption

1. Alice gets Bob's public key K_E = (n, e).

2. Represents the message as a number m between 0 and n-1.

3. Computes

$c = m^e \ mod \ n$

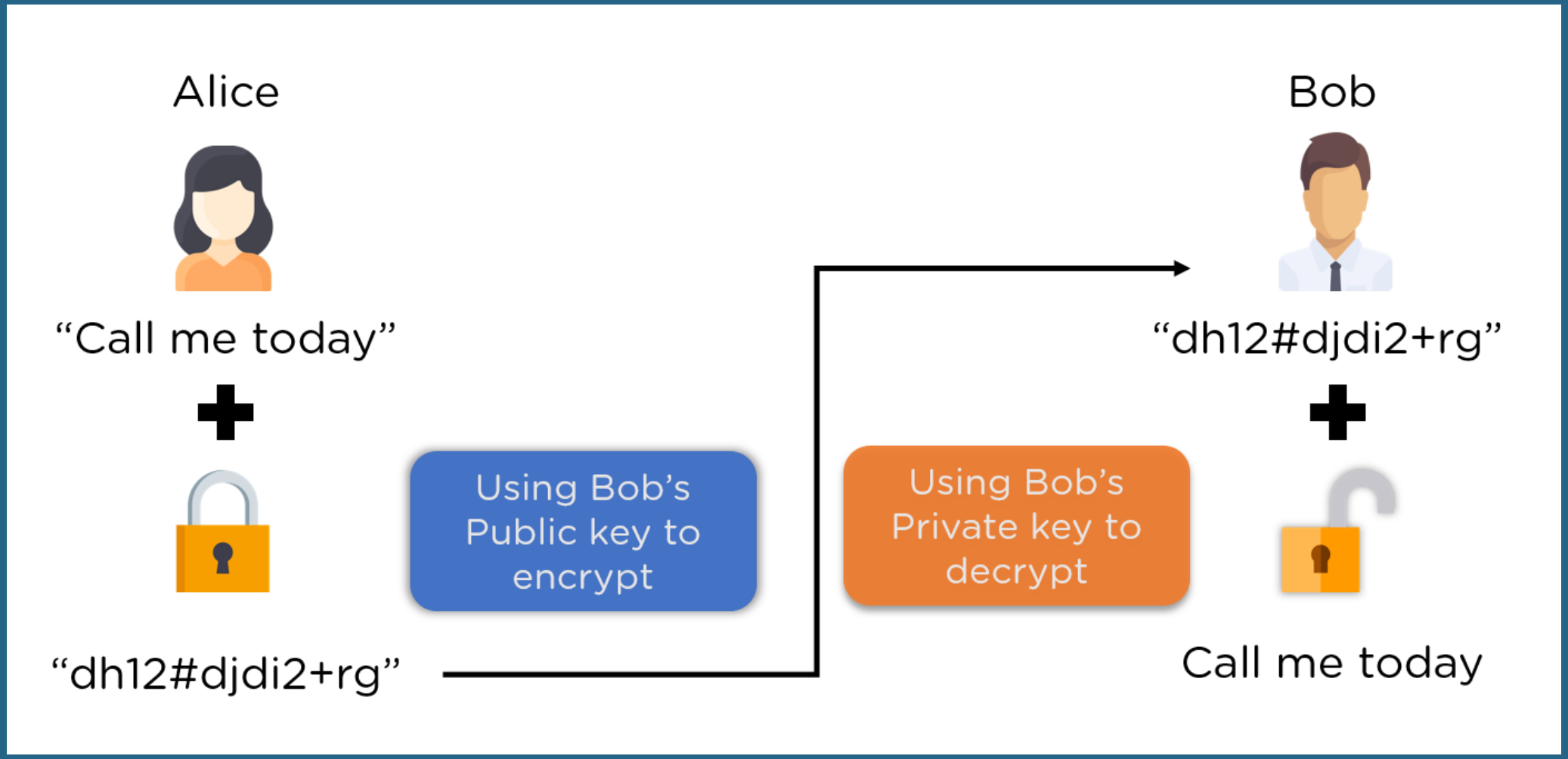
4. Alice sends the ciphertext c to Bob.

Decryption

Bob uses the private key

$K_D = d$ to get the message $m = c^d \ mod \ n$

Idea


Alice
Bob
“Call me today”
“dh12#djdi2+rg”
Using Bob’s Public key to encrypt
Using Bob’s Private key to decrypt
“dh12#djdi2+rg”
Call me today

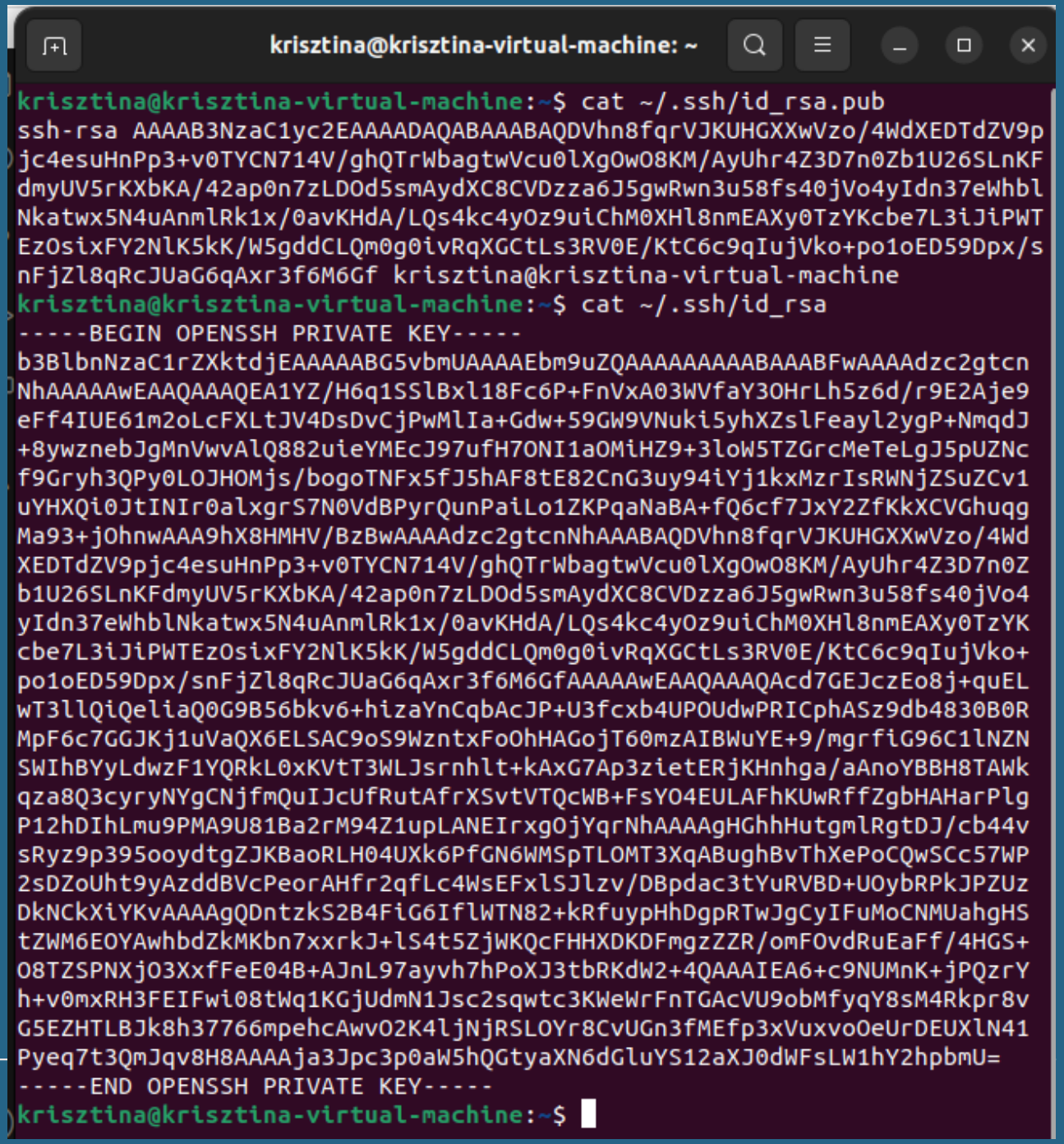
OpenSSH

- OpenSSH (Open Secure Shell) is a widely-used implementation of the SSH (Secure Shell) protocol, providing encrypted communication over a network.
- OpenSSH with RSA key pairs is used for secure and authenticated communication, remote login, and file transfer between systems.

Passwordless login with RSA:

```
ssh-keygen –t rsa –b 2048
ssh-copy-id username@ip
ssh username@ip
```

Keys generated using OpenSSH



Where is RSA used?

- *Secure Communication* – RSA employed in protocols like SSL/TLS to secure communication over the internet. It encrypts data during transmission, ensuring that sensitive data remains confidential.
- *Secure Shell (SSH)* – RSA is commonly used for secure remote login and command execution. Users can authenticate themselves to a remote server using RSA key pairs, enhancing security compared to password-based authentication.
- *VPNs* – RSA is often a part of key exchange mechanisms in VPN protocols.

DEMO

References

- N. Koblitz, A Course in Number Theory and Cryptography, Springer, 1994.

- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997. Centre For Applied Cryptographic Research: The University of Waterloo (uwaterloo.ca)

- C. Paar, J. Pelzl, Understanding Cryptography, Springer, 2009

- OpenSSH Server | Ubuntu