

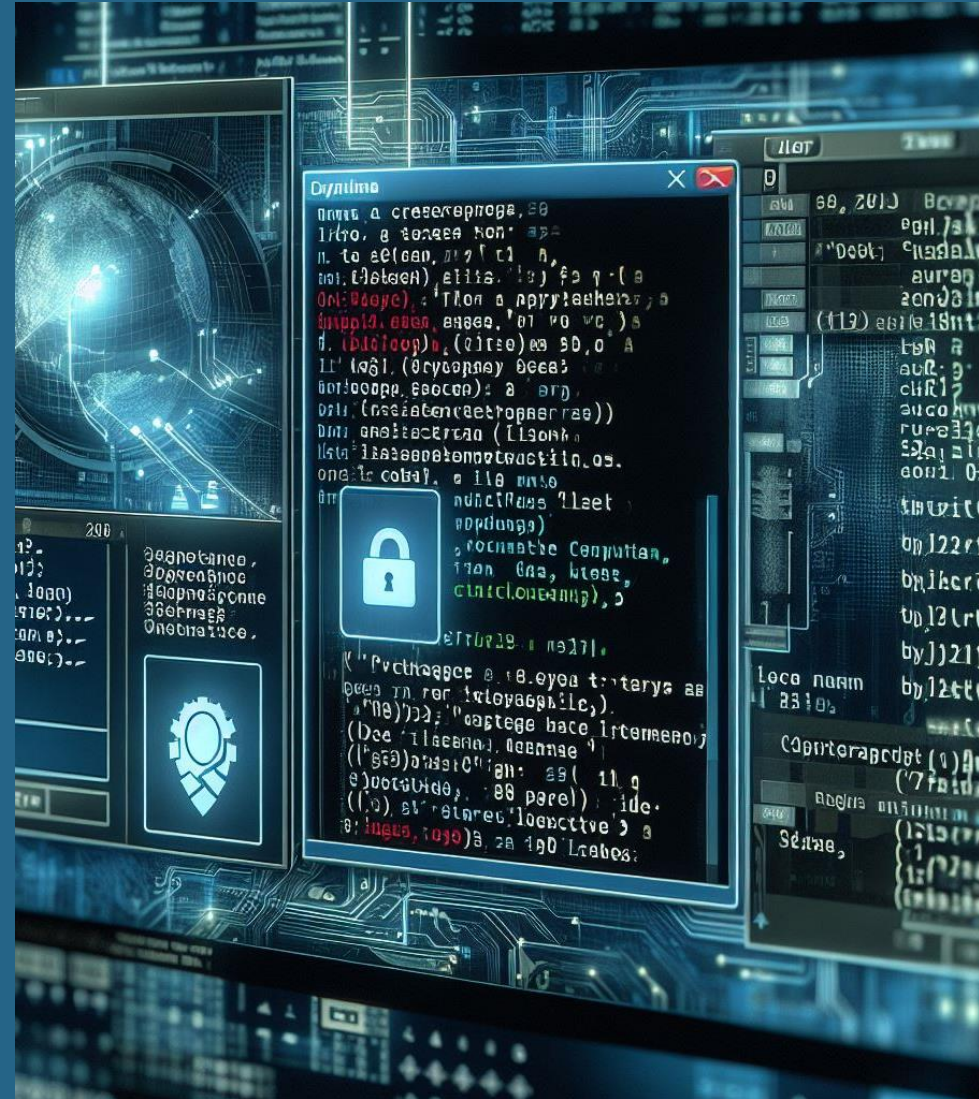
Public Key Cryptosystems

RSA

Horvath Krisztina-Aliz

Contents

1. Introduction
2. RSA Algorithm
3. OpenSSH
4. Conclusions
5. Demo



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 $c = m^e \bmod n$



4. Alice sends the ciphertext c to Bob.

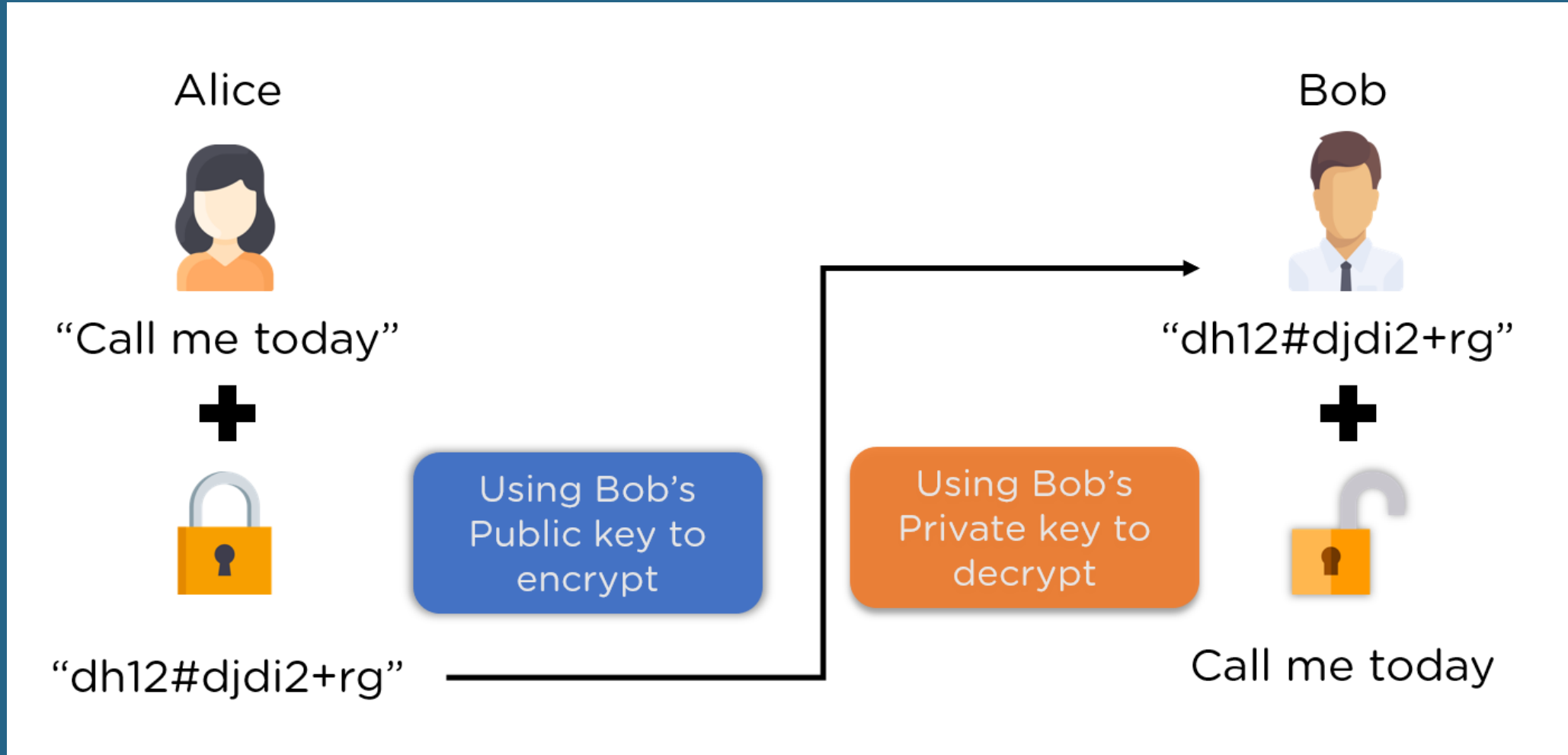
Decryption



Bob uses the private key

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

Idea



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

```
krisztina@krisztina-virtual-machine: ~  
krisztina@krisztina-virtual-machine:~$ cat ~/.ssh/id_rsa.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAQDVhn8fqrVJKUHGXXwVzo/4WdXEDTdZV9p  
jc4esuHnPP3+v0TYCN714V/ghQTrWbagtwVcu0lXg0w08KM/AyUhr4Z3D7n0Zb1U26SLnKF  
dmyUV5rKXbKA/42ap0n7zLD0d5smAydXC8CVDzza6J5gwRwn3u58fs40jVo4yIdn37eWhbl  
Nkatwx5N4uAnmlRk1x/0avKHdA/LQs4kc4yOz9uicHM0XHL8nmEAXy0TzYKcbe7L3iJiPWT  
Ez0sixFY2NlK5kK/W5gddCLQm0g0ivRqXGcTls3RV0E/KtC6c9qIujVko+po1oED59Dpx/s  
nFjZl8qRcJUaG6qAxx3f6M6Gf krisztina@krisztina-virtual-machine  
krisztina@krisztina-virtual-machine:~$ cat ~/.ssh/id_rsa  
-----BEGIN OPENSSH PRIVATE KEY-----  
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAAEbm9uZQAAAAAABAAABFwAAAAAdzc2gtcn  
NhAAAAAwEAAQAAQEA1YZ/H6q1SSlBxl18Fc6P+FnVxA03WVfaY30HrLh5z6d/r9E2Aje9  
eFf4IUE61m2oLcFXLtJV4DsDvcjPwMlIa+Gdw+59GW9VNuki5yhXZslFeayl2ygP+NmqdJ  
+8ywnzbJgMnVwvAlQ882uieYMEcJ97ufH70NI1a0MiHZ9+3loW5TZGrcMeTeLgJ5pUZnc  
f9Gryh3QPy0LOJHOMjs/bogoTNfx5fJ5hAF8tE82CnG3uy94iYj1kxMzrIsRWNjZSuZCv1  
uYHXQi0JtINIr0alxgrS7N0VdBPyrQunPailo1ZKPqaNaBA+fQ6cf7JxY2ZfKkXCVGhuqg  
Ma93+j0hnwAAA9hX8MHMV/BzBwAAAAAdzc2gtcnNhAAABAQDVhn8fqrVJKUHGXXwVzo/4Wd  
XEDTdZV9pjC4esuHnPP3+v0TYCN714V/ghQTrWbagtwVcu0lXg0w08KM/AyUhr4Z3D7n0Z  
b1U26SLnKFdmyUV5rKXbKA/42ap0n7zLD0d5smAydXC8CVDzza6J5gwRwn3u58fs40jVo4  
yIdn37eWhblNkatwx5N4uAnmlRk1x/0avKHdA/LQs4kc4yOz9uicHM0XHL8nmEAXy0TzYK  
cbe7L3iJiPWTEz0sixFY2NlK5kK/W5gddCLQm0g0ivRqXGcTls3RV0E/KtC6c9qIujVko+  
po1oED59Dpx/snFjZl8qRcJUaG6qAxx3f6M6GfAAAAAwEAAQAAQAc7GEJczEo8j+quEL  
wT3llQiQeliaQ0G9B56bkv6+hizaYnCbAcJP+U3fcxb4UPOUdwPRICphASz9db4830B0R  
MpF6c7GGJKj1uVaQX6ELSAC9oS9WzntxFo0hHAGojT60mzAIBWuYE+9/mgrfiG96C1lNZN  
SWIhBYyLdwzF1YQRkL0xKVtT3WLJsrnhlt+kAxG7Ap3zietERjKHnhga/aAnoYBBH8TAWk  
qza8Q3cyryNYgCNjfmQuIJcUfRutaFrXSvtVTQcWB+FsY04EULAFhKUwRffZgbHAHarPlg  
P12hDIhLmu9PMA9U81Ba2rM94Z1upLANEIrXg0jYqrNhAAAAGHGhhHutgmLRgtDJ/cb44v  
sRyz9p395ooydtgZJKBaoRLH04UXk6PfGN6WMSpTLOMT3XqABughBvThXePoCQwSCc57WP  
2sDZoUht9yAzddBVcPeorAHfr2qfLc4WSEfxLSJlZv/DBpdac3tYuRVBD+U0yBRPkJPZUZ  
DkNckXiYKvAAAAGQDntzks2B4FiG6IfLWTN82+kRfuypHhDgprTwJgCyIFuMoCNMUahgHS  
tZWM6EOYAwhbdZkMKbn7xxrkJ+lS4t5ZjWKQcFHHXDKDFmgZZR/omFOvdrUEaFf/4HGS+  
08TZSPNXj03XxfFeE04B+AJnL97ayvh7hPoXJ3tBRkdW2+4QAAAEIA6+c9NUMNk+jPQzrY  
h+v0mxRH3FEIFwi08tWq1KGjUdmN1Jsc2sqwtc3KWeWrFnTGAcVU9obMfyqY8sM4Rkpr8v  
G5EZHTLBjk8h3776mpehcAwv02K4lJnJrSLOYr8CvUGn3fMEfp3xVuxvo0eUrDEUXlN41  
Pyeq7t3QmJqv8H8AAAAja3Jpc3p0aw5hQGtyaXN6dGluYS12aXJ0dWFsLW1hY2hpbmU=  
-----END OPENSSH PRIVATE KEY-----  
krisztina@krisztina-virtual-machine:~$
```



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](#)
-