15.10 Public Key Authentication

As you study this section, answer the following questions:

- What is an MD5 checksum, and how is it used in public key authentication?
- Which file configures the server to accept public key authentication?
- Which keys are generated by the **ssh-keygen** command when you use the **-t rsa** option?
- Which utility should you use to copy encryption keys between Linux systems?
- When is the **~/authorized_keys** file used?
- How can you configure a client to automatically provide the private key passphrase when establishing an SSH session?

Key terms for this section include the following:

Term	Definition
Public key authentication	In lieu of a username and password, public key authentication uses a message that is encrypted and decrypted with different keys.
Public key	Public keys are public and should be distributed to all hosts with which the entity wants to communicate securely.
Private Key	Private keys are secret and known only to their owners.
Digital signature	A digital signature uses an asymmetric key pair to allow a sender's identity to be verified by a recipient.
Message digest	A hash value used to help verify the integrity of messages sent.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Linux Pro	4.3 Monitor and manage system access • Manage remote connections

CompTIA Linux+	2.3 Given a scenario, create, modify, and redirect files.
	• File and directory operations
	  ◦ scp
	3.2 Given a scenario, configure and implement appropriate access and authentication methods.
	• SSH
	  ◦ authorized_keys
	  ◦ sshd.conf

- id_rsa
- User-specific access
- ssh-copy-id
- ssh-keygen
- ssh-add

- PKI
  - Self-signed
  - Private keys
  - Public keys
  - Hashing
  - Digital signatures
  - Message digest

3.6 Given a scenario, backup, restore, and compress files.

- Off-site/off-system storage
  - scp
- Integrity checks
  - MD5

Copyright © 2022 TestOut Corporation All rights reserved.