Cryptography Tools Cheat Sheet

This document covers common cryptography tools, their platforms, use cases, and example commands/steps for usage.

# MD5HashCalc

Platform: Windows

Description: A lightweight tool to generate and verify MD5 hashes.

Usage:

* Step 1: Open MD5HashCalc and browse the file you want to check.
* Step 2: Click 'Calculate' to generate the MD5 hash and compare with the provided hash.

# BCTextEncoder

Platform: Windows

Description: Encrypt and decrypt text messages using symmetric encryption (password-based).

Usage:

* Step 1: Open BCTextEncoder and enter the text you want to encrypt.
* Step 2: Provide a password and click 'Encrypt'; use the same password to decrypt.

# CryptoForge

Platform: Windows

Description: File and folder encryption utility supporting strong algorithms (AES, Blowfish, etc.).

Usage:

* Step 1: Right-click on a file/folder and choose 'Encrypt with CryptoForge'.
* Step 2: Provide your encryption key/password; decrypt the same way with 'Decrypt'.

# PerformDiskEncryption

Platform: General/Conceptual

Description: Generic full-disk encryption process applied by different tools.

Usage:

* Step 1: Use a disk encryption utility like BitLocker or VeraCrypt.
* Step 2: Configure encryption key and encrypt the entire drive.

# BitLocker

Platform: Windows

Description: Microsoft’s built-in full-disk encryption tool for protecting entire drives.

Usage:

* Command 1: Enable BitLocker: manage-bde -on C:
* Command 2: Check status: manage-bde -status

# LUKS

Platform: Linux

Description: Linux Unified Key Setup (LUKS) for disk encryption on Linux systems.

Usage:

* Command 1: Encrypt a partition: cryptsetup luksFormat /dev/sdX
* Command 2: Open it: cryptsetup luksOpen /dev/sdX secure\_partition

# VeraCrypt

Platform: Windows/Linux/macOS

Description: Popular open-source disk encryption tool, successor to TrueCrypt.

Usage:

* Step 1: Create a new volume via VeraCrypt GUI (select encryption algorithm).
* Step 2: Mount the volume with your password/keyfile.