7-ZIP: https://www.7-zip.org/7z.html

7-Zip also supports encryption with AES-256 algorithm. This algorithm uses cipher key with length of 256 bits.

To create that key 7-Zip uses derivation function based on SHA-256 hash algorithm. A key derivation function produces a derived key from text password defined by user. For increasing the cost of exhaustive search for passwords 7-Zip uses big number of iterations to produce cipher key from text password.

Microsoft Office: https://en.wikipedia.org/wiki/Microsoft_Office_password_protection

Microsoft Office password protection is a security feature to protect Microsoft Office (Word, Excel, PowerPoint) documents with a user-provided password. As of Office 2007, this uses modern encryption; earlier versions used weaker systems and are not considered secure.

Office 2007–2013 employed 128-bit key AES password protection which remains secure.

Office 2016 employed 256-bit key AES password protection which also remains secure.

The Office 97–2003 password protection used 40-bit key RC4 which contains multiple vulnerabilities rendering it insecure.

Skype: https://support.skype.com/en/faq/fa31/does-skype-use-encryption

For instant messages, we use TLS (transport-level security) to encrypt your messages between your Skype client and the chat service in our cloud, or AES (Advanced Encryption Standard) when sent directly between two Skype clients. Most messages are sent both ways, but in the future it will only be sent via our cloud to provide the optimal user experience.

Voice messages are encrypted when they're delivered to you. However, after you have listened to a voice message, it is transferred from our servers to your local machine, where it is stored as an unencrypted file.

Skype uses the AES (Advanced Encryption Standard*), also known as Rijndael, which is used by the US Government to protect sensitive information, and Skype has for some time always used the strong 256-bit encryption. User public keys are certified by the Skype server at login using 1536 or 2048-bit RSA certificates.

Apple: https://support.apple.com/hu-hu/guide/security/secf6276da8a/web

Apple uses a technology called Data Protection to protect data stored in flash storage on the devices that feature an Apple SoC such as iPhone, iPad, Apple Watch, Apple TV, and a Mac with Apple silicon.

Every time a file on the data volume is created, Data Protection creates a new 256-bit key (the per-file key) and gives it to the hardware AES Engine, which uses the key to encrypt the file as it is written to flash storage. On A14 and M1 devices, the encryption uses AES-256 in XTS mode where the 256-bit per-file-key goes through a Key Derivation Function (NIST Special Publication 800-108) to derive a 256-bit tweak and a 256-bit cipher key. The hardware generations of A9 through A13, S5, and S6 use AES-128 in XTS mode where the 256-bit per file key was split to provide a 128-bit tweak and a 128-bit cipher key.

Dropbox: https://www.virtru.com/blog/dropbox-encryption/

Dropbox encryption uses 256-bit AES keys to protect files at rest, and encrypts data in motion with 128-bit AES SSL/TLS encryption or better.

Google Drive:

Google Drive encryption is similar; files in motion are protected using 256-bit SSL/TLS encryption, while those at rest are encrypted with 128-bit AES keys.

OneDrive: https://support.microsoft.com/en-us/office/how-onedrive-safeguards-your-data-in-the-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1

-Protected in transit

When data transits into the service from clients, and between datacenters, it's protected using transport layer security (TLS) encryption. We only permit secure access. We won't allow authenticated connections over HTTP, but instead redirect to HTTPS.

-Protected at rest

Content protection: Each file is encrypted at rest with a unique AES256 key. These unique keys are encrypted with a set of master keys that are stored in Azure Key Vault.