Telegram官网

Telegram官网隐私加密说明页，介绍普通聊天与秘密聊天的加密差异，以及 AES、RSA 与 Diffie-Hellman 组合加密机制。

https://tao-zhifeiji.ltd/

Telegram官网

理解普通聊天与秘密聊天的加密差异，以及 AES、RSA 与 Diffie-Hellman 如何组合成可靠的消息保护机制。

普通聊天 vs 秘密聊天：加密差异

Telegram官网隐私加密说明页旨在帮助用户理解两类聊天模式背后的安全逻辑。普通聊天采用客户端-服务器加密，数据在传输中加密，但服务器可解密以支持多设备同步；秘密聊天则使用端到端加密，只有通信双方能够读取信息。

普通聊天

默认启用，消息在设备与服务器之间加密传输。服务器可解密并存储，以便在多个设备上同步。适合日常沟通，但不适合高度敏感信息。

秘密聊天

端到端加密，消息仅存在于发送方与接收方设备上。支持自毁定时器，不经过服务器存储，无法转发或截图提醒。适合机密对话。

组合加密机制

秘密聊天使用 Diffie-Hellman 密钥交换建立共享密钥，再结合 AES 对称加密与 RSA 身份验证，形成多层防护。

加密机制图解

组合加密机制：四步理解

密钥交换

通信双方使用 Diffie-Hellman 算法在公开通道协商出一个只有双方知道的共享密钥，无需预先共享秘密。

身份验证

RSA 非对称加密用于验证对方身份，确保与你通信的是预期的人，而非中间人。

消息加密

利用协商出的共享密钥，AES 对称加密算法快速加密消息内容，保证机密性和完整性。

端到端保护

秘密聊天中，加密后的消息仅在发送与接收设备上解密，服务器只传递密文。

实用隐私建议

敏感对话用秘密聊天

涉及密码、财务或个人隐私时，优先开启秘密聊天，并设置自毁定时器。

验证密钥指纹

与对方比对加密密钥指纹，可降低中间人攻击风险。

谨慎使用云同步

普通聊天会同步到云端，若设备丢失可能泄露历史消息。

保持应用更新

及时更新 Telegram 客户端，修复已知安全漏洞。

想深入了解 Telegram 加密机制？

访问 Telegram 官方帮助中心，获取最新技术文档与安全说明。