Firebase provides data security and encryption for its various services. Specifically with respect to data encryption, Firebase uses the following primary methods to protect data in storage and in transit:

1. **Encryption of Data Transmission**:
   * Firebase uses the HTTPS protocol to encrypt all communications between the client and server. This means that all data transmitted through Firebase is encrypted in transit to prevent data eavesdropping.
   * For data using Firebase Cloud Messaging (FCM), Firebase also ensures that messages transmitted between the server and the client travel over a secure channel.
2. **Encryption of data storage**:
   * Across Firebase's storage solutions, such as Firebase Realtime Database and Cloud Firestore, data stored on Google's servers is encrypted on the server side. This includes encryption of both at-rest data storage and backup data.
   * Firebase encrypts data by default using Google's standard encryption technologies, such as AES256 or higher.
3. **User data security**:
   * Firebase Authentication provides user authentication with support for multiple login methods (e.g., passwords, social media accounts, phone numbers, etc.) and encrypts user login information to protect user credentials and privacy.
   * Firebase also provides the option to configure security rules, allowing developers to restrict access to data as needed by the application.