Найти как можно больше проблем, предложить возможные исправления.

Мобильное приложение, скаченное с MobileStore.

Цель – привязать (pair) телефон к интерактивному телевизионному экрану в самолёте.

На экране после привязки отображается информация о пассажире, статусе полёта. Управление экраном после привязывания производится через приложение.

После посадки на место пассажир самолёта видит перед собой экран. При запуске процесса привязывания телефона на нём отображается четырёхзначный пин-код (целые числа), которые необходимо ввести в приложении. После этого, значение пин-кода хэшируется с использованием SHA-256 для получения ключа .

После этого на экране отображается SSID wifi точки для подключения телефона.

После подключения к WiFi устанавливается соединение между телефоном и экраном. Используя эфемерный Диффи-Хееллман по модулю 768 бит генерируется общий ключ , который затем складывается по модулю 2 с ключом , при этом лишние биты отбрасывается. Полученный ключ используется для шифрования всех данных между телефоном и экраном, используя AES-128 в режиме ECB. .

Найти как можно больше проблем, предложить возможные исправления.

Мобильное приложение, скаченное с MobileStore.

Цель – привязать (pair) телефон к интерактивному телевизионному экрану в самолёте.

На экране после привязки отображается информация о пассажире, статусе полёта. Управление экраном после привязывания производится через приложение.

После посадки на место пассажир самолёта видит перед собой экран. При запуске процесса привязывания телефона на нём отображается четырёхзначный пин-код (целые числа), которые необходимо ввести в приложении. После этого, значение пин-кода хэшируется с использованием SHA-256 для получения ключа .

После этого на экране отображается SSID wifi точки для подключения телефона.

После подключения к WiFi устанавливается соединение между телефоном и экраном. Используя эфемерный Диффи-Хееллман по модулю 768 бит генерируется общий ключ , который затем складывается по модулю 2 с ключом , при этом лишние биты отбрасывается. Полученный ключ используется для шифрования всех данных между телефоном и экраном, используя AES-128 в режиме ECB. .