1. WEP 共享密钥认证包括哪些主要步骤？

整个认证过程包括四个步骤

① 客户端向接入点，发送身份验证请求

② 接入点会回复明文质询

③ 客户端使用配置的 WEP 密钥对质询文本进行加密，然后在另一个身份验证请求中将其送回

④ 接入点，解密响应，如果与质询文本匹配，则接入点将发送肯定答复

2. 802.11i 定义了哪些安全服务？

IEEE 802.11i 关注了无线接入点和无线工作站点之间的安全通信，引入了健壮安全网络的概念，定义了以下安全服务

①认证：定义用户和网络的交互，以提供相互认证，并生成用于 STA 和 AP 之间无线通信的短期密钥

②访问控制：对认证功能的增强，能与多种认证协议协同工作

③带消息完整性的机密性：MAC 层数据与消息完整性校验码一起加密以提供机密性与完整性

3 802.11i 的认证过程包括哪些阶段？

认证模型包含三个实体：请求者：STA、认证者：AP、认证服务器：AS，认证过程包括：

① 连接到 AS：STA 向它的 AP 发送一个请求以连接到 AS，AP 识别这个请求并给 AS 发送一个访问请求

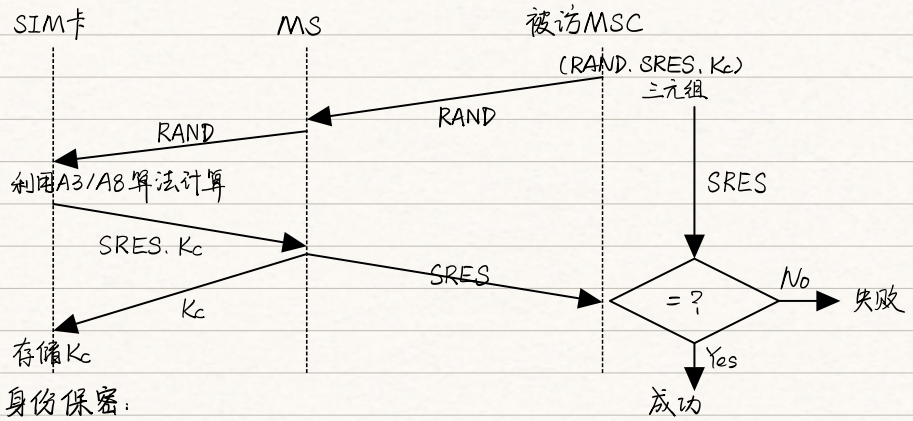
② EAP 交换：这个交换让 STA 和 AS 相互授权

③ 安全密钥分发：一旦认证完成，AS 和 STA 产生一个主会话密钥（MSK），此密钥也被称为 AAA 密钥，STA 和 AP 进行安全通信所需的加密密钥都从 MSK 产生

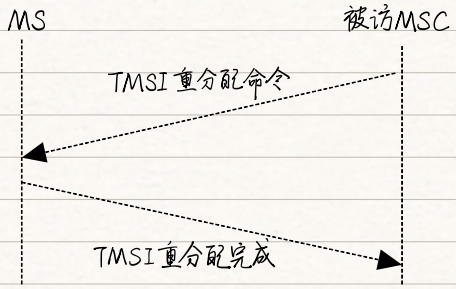
4. GSM 安全包括哪些安全功能？

GSM 的安全机制包括了以下几方面的功能

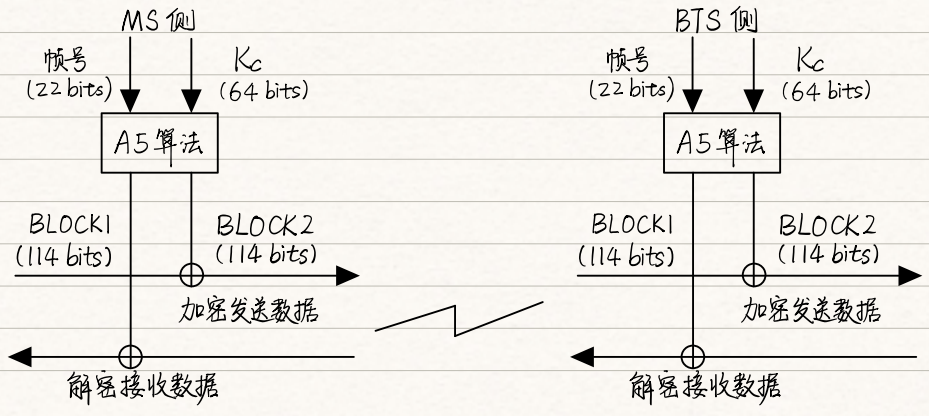
① 用户身份认证：



② 用户身份保密：



③ 用户数据保密以及信令数据保密



5 简述3GPP的安全总体结构

① 网络接入安全：提供安全接入3G服务网的机制并抵御对无线链路的攻击，这一部分的功能包括：用户身份保密、认证和密钥分配、数据加密和完整等.

② 网络域安全：保证网内信令的安全传送并抵御对有线网络(核心网部分)的攻击

③ 用户域安全：主要保证对移动台的安全接入，包括用户与智能卡之间的认证、智能卡与终端间的认证及其链路的保护

④ 应用域安全：使用户域与服务提供商的应用程序能够安全地交换信息.

⑤ 安全特性的可视性及可配置能力：主要指用户能获知安全特性是否在使用以及服务提供商提供的服务是否需要以安全服务为基础

6. 简述5G安全架构与4G安全架构的不同之处

① 加强了网络接入安全，增加了非3GPP接入，同时增强了AKA协议，堵上了拜访域欺骗归属域的漏洞

② 面向垂直行业需求，新增了二次认证，在满足垂直行业差异化需求的同时增强了安全性

③ 新增了SBA域的安全，考虑了服务化网元的安全交互

④ 应用域安全，新增了空口可选的完整性保护手段