《现代计算机信息安全理论基础》答题卡

I. 答题说明

1. 请正确填写考生信息。
2. 请以标准 Markdown 语法在本文件尾部填写每一道题的答案。

II. 考生信息

.	.
姓名	XXXX
部门	研发部

III. 答题处

1. 请以文字描述以下术语的定义：（12分）
    - 加密：通过特定算法，将明文转换为第三方无法理解密文。（2分）
    - 解密：通过特定算法，将密文还原为明文。（2分）
    - 签名：通过特定算法，对一段数据的散列值进行处理生成不可伪造的值。（2分）
    - 校验：通过特定算法，对签名的值进行校验。（2分）
    - 信源：生成信息的源头实体。（2分）
    - 信道：信息传输的介质、通道。（2分）
2. 加密算法分为哪两大类？AES 算法和 RSA 算法分别属于哪一类？哪一类算法可以用来签名和校验？（8 分）
    - 对称加密算法和非对称加密算法；（2分）
    - AES 是对称加密算法，RSA 是非对称加密算法；（2分）
    - 散列算法，非对称加密算法都可用于签名和校验。（4分）
3. Enigma 密码机，加密和解密的操作完全一致，是基于什么原理？（8分）
    - Enigma 密码机使用通过转轮机制产生大量换字表，每个转轮组位置就是一个换字表，每加密完一个字符，转轮组步进一位，产生一张新的换字表。（3分）
    - 字符正向通过转轮就是加密过程，反向则是解密过程，而反射板（一个自反函数）将这两个过程合而为一，先经过加密过程，然后通过反射板，得到另一个字符，走一次解密过程。（5分）

    加密流程：

```
A -> 转轮1 -> N -> 转轮2 -> O -> 转轮3 -> X ->
                                          反射板
G <- 转轮1 <- E <- 转轮2 <- C <- 转轮3 <- T <-
```

解密流程

```
G -> 转轮1 -> E -> 转轮2 -> C -> 转轮3 -> T ->
                                          反射板
A <- 转轮1 <- N <- 转轮2 <- O <- 转轮3 <- X <-
```

4. DDoS 攻击会造成什么影响？它和 CC 攻击的区别是什么？（10分）
    - DDoS 攻击会造成目标设备流量拥堵（3分），甚至在处理大量数据包的过程中，系统无法及时响应，而造成宕机（3分）。
    - DDoS 是传输层攻击，CC 攻击是应用层攻击。（4分）
5. 浏览器的跨域限制，制止了哪类攻击？这类攻击的原理是什么？如何完全规避这类攻击？（12分）
    - CSRF 攻击。（2分）
    - 原理是利用基于目标系统的接口参数设计缺陷和 Cookies 传递机制，在用户未知的情况下（如利用IMG标签）触发目标接口。（6分）
    - 防范方式有如：不使用 Cookies 验证、使用 HTTP 请求头 Referer 进行校验等。（4分）
6. HMAC 算法通常用在哪些操作上？为什么？如果用于保护信源安全，它有什么缺点？如何防范？（16分）
    - 身份验证、数据真实性验证。（4分）
    - HMAC 使用散列算法配合秘钥的生成数字签名，在未知秘钥的前提下，短时间内很难对签名结果产生一致性冲突。（4分）
    - 缺点是会遭到重试攻击，且必须提前协商秘钥。（4分）
    - 方法如添加短暂的签名有效期，或者增加累加计数器防止重复请求，或者改用 TLS 协议。（4分）
7. TLS 协议的作用是什么？证书验证流程是什么样的？请画图解释 TLS 协议的基本流程。并举例说明一种针对 TLS 的攻击方式。（24分）
    - 可以同时确保信源和信道安全。（3分）
    - 证书验证流程是从二级CA证书开始，使用上级证书里的公钥对该证书进行非对称散列签名校验，直到把每一级证书都校验完毕。（4分）
    - 图省略，自行脑补。（12分）
    - 例：入侵路由器，劫持子网设备的 DNS，使用伪造证书伪装成远程服务器，窃听网络通信内容。(5分)