18、添加规则，允许通往 192.168.0.2 的 SSH 连接的 IPtables 指令

答：iptables -A forword -p tcp -d 192.168.0.2 -dport 22 -j accept

【注：IPtables 这个部分在教材中有出现，也属于防火墙的实践应用的一部分内容，可以作为考察点。但是，如果单纯考编写规则，那么题目中肯定要出现参数含义，这样题目变得很简单。所以个人认为，这个知识点不容易出大题，有可能出在填空选择上，需要考生自己把握。】

19、在访问控制技术中，ACL 方式是实现 DAC 策略的最好方式，下表是客体 File1 的带通配符“*”的 ACL，下面那些是错误的（ ）

Joann.prog.REW	*.prog.R	Zbs.*.RE	*.*.NULL

A、组 prog 中只有 Joann 有 REW 权限，prog 组其他只有 R 权限

B、任意组中，用户 Zbs 都有 RE 权限

C、无论哪个组，任何用户都没有权限

D、组 prog 的所有用户都只有 R 权限

答：C、D 注意 ACL 含义：File(客体)->Jonna(主体)->prog(组)->权限

20、AES 的分组长度是（ ）位，其安全性至少相当于（ ）

答：128、三重 DES

【注：这个知识点在对称密钥加密的后面介绍 AES 加密算法时候有提到。】

21、简单说明对称密钥与公开密钥的区别和优缺点。

答：一、区别：对称密钥双方使用一个事先协商的密钥，公开密钥中，每个用户具有一个公钥与一个私钥，公钥公开

二、优缺点：1）对称密钥：密钥管理麻烦，n 个用户需要管理 n*(n-1)/2 对密钥，加密速度快

2）公开密钥：运算速度慢，产生密钥复杂，安全性要求尽可能大的密钥

22、试比较 DES 与 RSA

答：一、DES 在计算效率上优于 RSA，可用软件和硬件加速处理，RSA 要大整数乘幂求模运算，速度较慢（计算效率）

二、RSA 比 DES 适合大规模网络应用。DES 是对称密钥，密钥管理麻烦（密钥管理）

三、DES 算法由于密钥为 56bits，可被破解，RSA 使用大整数分解的思想，在长密钥下较难破解（安全性）

四、RSA 可以应用在数字签名和身份认证上，DES 无法支持（应用场景）

【注：DES 是对称密钥的代表，RSA 是公开密钥的代表，要注意两者的区别以及优缺点，理解两种不同密钥体制，以及两种典型的加密算法用到的理论基础。】

23、用费马定理计算 $3^{201} \bmod 11$

答:,

$$\gcd(3,11)=1 \Rightarrow 3^{10} \bmod 11 = 1$$

$$3^{201} \bmod 11 = 3^{200} * 3 \bmod 11 = ((3^{200} \bmod 11) * (3 \bmod 11)) \bmod 11$$
$$= (((3^{10} \bmod 11)^{20} \bmod 11) * (3 \bmod 11)) \bmod 11$$
$$= 3 \bmod 11 = 3$$

【注：了解即可，主要了解一下费马定理 $3^{n-1} \bmod (n-1) = 1$，在求模计算上方便。并且要知道快速求模方法，2019 年 837 求 RSA 计算中就出现求模运算。】

24、设哈希函数有 128 位输出,如果 H 的 K 个随机数输入中至少有两个产生相同输出概率大于 0.5，则 K 约等于（ ）

A、2^128　　B、2^64　　C、2^32　　D、2^256

答：B

【注：生日悖论（信息安全导论 P41），n 位长度的散列值，可能发生一次碰撞次数不是 2^n，而是大于 2^(n/2)次数，所以选 B。具体的哈希碰撞概率，见后面推导。】

25、下列哪种算法只能用于数字签名（ ）

A、DES　B、DSA　C、RSA　D、SHA

答：B

【注：由 NIST 提出的数字签名标准，DSA 不是标准公钥密码，只能提供数字签名功能。见书 P45 页最下面。这属于比较偏的知识点，再这边归纳，有个影响以防万一。】

26、填空题：PKI 采用证书管理公钥，通过（ ）把用户公钥和用户信息绑定。PKI 公钥基础设施就是提供（ ）和（ ）的服务平台。

答：第三方可信任 CA、公钥加密、数字签名

【注：单纯的公钥加密体系是无法支撑大规模的网络应用的，这就需要公钥基础设施 PKI 来完成。所以考察公钥加密还可以从 PKI 基础设施的角度入手，包括 PKI 体系结构，应用什么技术，证书链，证书的验证等等问题。其中个人认为，PKI 体系结构的 CA 和证书链的验证原理是比较重点的，也是没有出过题目的。】

27、给定元素 p=3，q=11 用 RSA 算法生成一对密钥，（1）若选公钥 e=3，计算私钥 d 的值。（2）对于明文 m=5 加密求 c 的值

答：（1）$\Phi(n)=2*10=20$，$n=p*q=33$，$d*e \bmod \Phi(n)=1 \Rightarrow d=7$　（2）$m^e \bmod n=5^3 \bmod 37=26$

【注：RSA 的公私计算，以及根据公钥反推私钥的计算都要进行掌握，计算题一般都是从 RSA、DH 这两部分来出】

28、填空题：数字证书中内容包括证书版本、（ ）、（ ）、（ ）、（ ）

答：签名算法、有效期、主体公钥信息、证书颁发者的数字签名

【注：一般来说不会要求把数字证书的内容都记下，但是 2019 年 837 的计算机网络部分考题有要求写出 UDP 头字段，所以会不会在信息安全导论部分也这么出题？】