No.
Date. / /

5.10

∵ $n=pq$，且p和q都是素数，$\gcd(x,n)$可以是p、q和n（除去$x\in Z_n^*$）

①若$\gcd(x,n)=p$，则 $x\equiv 0 \pmod p$，且$\gcd(x,q)=1$

我们需要证明$x^{ab}\equiv x \pmod p$和$x^{ab}\equiv x \pmod q$

前者易知成立，对于后者：∵ $\gcd(x,q)=1$，且$ab\equiv 1 \pmod{(p-1)(q-1)}$

∴ $ab\equiv 1 \pmod{(q-1)}$

∴根据费马小定理 $x^{ab}\equiv x \pmod q$

∴由CRT，$x^{ab}\equiv x \pmod n$

②若$\gcd(x,n)=q$，同理可得$x^{ab}\equiv x \pmod n$

③若$\gcd(x,n)=n$，则$x\equiv 0 \pmod n$，则显然$x^{ab}\equiv 0\equiv x \pmod n$

∴综上，$d(e(x))=x$对任一$x\in Z_n$都成立

5.14

攻击者选择$\hat{y}=y\cdot e_k(r) \pmod n$，$r\in Z_n^*$

解密$\hat{y}$得到$\hat{x}=d_k(\hat{y})d_k(e_k(r))\equiv x\cdot r \pmod n$

则攻击者计算$x\equiv \hat{x}\cdot r^{-1} \pmod n$，从而得到x

∴RSA对于选择密文攻击是不安全的

5.34

(1) 证明 $half(y)=parity((y\times e_k(2)) \bmod n)$

$y\times e_k(2)=e_k(x)\times e_k(2)=e_k(2x) \pmod n$

1、$0\le x<\frac{n}{2}$，则$half(y)=0$，而2x为偶数 ∴ $parity(e_k(2x) \pmod n)=0$

2、$\frac{n}{2}\le x<n$，则$half(y)=1$，$2x\in[n,2n)$ ∴ $2x \pmod n=2x-n$

且n为奇数 ∴ $2x \pmod n$为奇数 ∴ $parity(e_k(2x) \pmod n)=1$

∴综上，$half(y)=parity((y\times e_k(2)) \bmod n)$

No.

Date. / /

(2)证明 $parity(y) = half((y \times e_k(2^{-1})) \bmod n$.

同理，$(y \times e_k(2^{-1}))(\bmod n) = e^{\frac{x}{2}}(\bmod n)$

1. 若x为偶数，则$parity(y)=0$。设$x=2k$（k为整数），则$\frac{x}{2}=k$，...

∵ $0 \le x < n$ ∴ $0 \le k < \frac{n}{2}$

∴ $half(e_k(k) \bmod n) = 0$

2. 若x为奇数，则$parity(y)=1$。设$x=2k+1$（$k \in Z$），则$\frac{x}{2}=k+2^{-1}$

∴ $0 \le k < \frac{n-2}{2}$

∴ $e_k(x \cdot 2^{-1}) = e_k((2k+1) \times \frac{n+1}{2}) = e_k(k+\frac{n+1}{2})$

∵ $\frac{n+1}{2} \le k+\frac{n+1}{2} < \frac{n-2}{2}+\frac{n+1}{2} = n-\frac{1}{2}$

∴ $half(y \times e_k(2^{-1})) = 1$

∴ 综上，$parity(y) = half((y \times e_k(2^{-1})) \bmod n$