Exercise_07

1.

- Authentication is required to identifies the customers.
- Access control is required to make sure that only paid customers can watch
- Data integrity is required to make sure the service is at good and legal condition

2.

(a) d = gcd(a,b).

The last remainder is 0, and the second to last remainder is d, so we get a sequence {0, d, kd, nkd+d, ...}. By observation, we a_n + a_{n+1} < a_{n+2}, so it increases faster than Fibonacci sequence, so the complexity is $O(logb)$.

(b) Considering the square-multiplication algorithm for RSA encryption, every multiplication operation needs $O(k^2)$ complexity where k is the text length and the algorithm needs $\log e$ multiplications. Thus, the time complexity is $O(k_2 \log e)$.

3.

If M doesn't have redundancy structure, it is susceptible to existential forgeries. Let (e, N) be the public signature verification key of RSA, then one can randomly choose a signature σ and compute the message $m = \sigma^e$(mod N). Applying a redundancy structure to messages, for example, hashing and padding prior to signing, the forged signatures would be useless so that the signature can be securely verified.

4.

If $|p - q|$ is too small, we can use Fermat factoring method to calculate p and q quickly.

The Fermat factoring method works as follows: for $a = \lceil\sqrt{n}\rceil, \lceil\sqrt{n}\rceil + 1, \lceil\sqrt{n}\rceil + 2, \ldots$, it checks whether n/a^2 is a perfect square; if so, it has factored nn.

We can analysis the running time of Fermat's method. Let $\epsilon = (p/\sqrt{n}) - 1$, so that $p = \sqrt{n}(1+\epsilon)$ and $q = \sqrt{n}/(1+\epsilon) = \sqrt{n}(1-\epsilon+\epsilon^2-\cdots)$. Fermat's method succeeds when $a = (p+q)/2 = \sqrt{n}(1+\epsilon^2/2-\cdots)$. In other words, it requires $\approx \sqrt{n}\epsilon^2/2$ iterations.

So, since $|p-q| \approx 2\sqrt{n}\epsilon$, if $|p-q| < 10000$, we can get that:

$$\{ 2\sqrt{n}\epsilon < 10000 \ \sqrt{n}\epsilon^2/2 = t$$

Then, we get get the conclusion that: $t < \frac{10^8\sqrt{N}}{2}$

So, p, q can be calculated in reasonable time, then the RSA could be broken in limited time.

5.

From the definition of the totient function, we have the relation:

$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = (n+1) - (p+q)$

Then easily follows that:

$(n+1) - \phi(n) = p + q$

$(n+1) - \phi(n) - p = q$

Since $n = pq$, so $p^2 - (n+1-\phi(n))p + n = 0$, this is a quadratic equation in p, with:

$$\begin{aligned} a &= \frac{1}{b} \\ &= -\frac{(n+1-\phi(n))}{c} \\ &= n \end{aligned}$$

$p = \frac{-b \pm \sqrt{|b|^2 - 4ac}}{2a} = \frac{(n+1-\phi(n)) \pm \sqrt{|n+1-\phi(n)|^2 - 4n}}{2}$

In conclusion, knowledge of $\phi(n)$ allows one to factor n in time $O(1)$. The other answers are equivalent.