Chapter 5

5.1 In CBC mode we have $c_i = E_K(c_{i-1} \oplus m_i)$. Decrypting both sides gives

$$D_K(c_i) = c_{i-1} \oplus m_i \Rightarrow m_i = D_K(c_i) \oplus c_{i-1}.$$

5.2 In a distinguishing attack we want to distinguish the keystream from a truly random sequence. Since a block cipher is an invertible function we have

$$E_K(x) \neq E_K(y) \quad \text{if } x \neq y,$$

otherwise decryption would not be deterministic. Since a block cipher in counter mode encrypts an incrementing counter, the keystream blocks will never repeat. In a truly random sequence, keysteam blocks can repeat. Thus, in the distinguishing attack we observe the keystream block and if they never repeat, the sequence is from the cipher. Otherwise it is random. The distinguisher can be written as

```
Input (a_1, a_2, a_3, ..., a_N)
if a_i = a_j for some i≠j
  output Random
else
  output Counter Mode
```

How many cipher blocks do we need to observe such that the probability for correct decision is significantly larger than 0.5? Assume that we have observed N m-bit blocks. A block can have one of $M = 2^m$ possible values. In a truly random sequence the probability that all blocks are distinct is

$$\left(1 - \frac{1}{M}\right)\left(1 - \frac{2}{M}\right)\cdots\left(1 - \frac{N-1}{M}\right) \approx \prod_{i=1}^{N-1} e^{\frac{-i}{M}} = e^{-\frac{1}{M}\sum_{i=1}^{N-1} i} = e^{\frac{-N(N-1)}{2M}}$$

since $1 - x \approx e^{-x}$ when x is small. Thus, the probability for at least one collision is

$$\epsilon \approx 1 - e^{\frac{-N(N-1)}{2M}} \Rightarrow \frac{-N(N-1)}{2M} \approx \ln(1-\epsilon) \Rightarrow N^2 - N \approx 2M \ln\frac{1}{1-\epsilon}.$$

If N is large, we can ignore the $-N$ term and we get

$$N \approx \sqrt{2M \ln\frac{1}{1-\epsilon}}.$$

The breaking point, when our distinguisher will have better probability than a random guess is when $\epsilon = 0.5$. This is reached when $N \approx 1.18\sqrt{M} = 1.18 \cdot 2^{32}$. If we want a higher probability, e.g., $\epsilon = 0.95$, we need to observe $N \approx 2.45\sqrt{M} = 2.45 \cdot 2^{32}$ keystream blocks. (In general, if we observe random samples from a uniform distribution of size M, we expect a collision after about $N = C\sqrt{M}$ samples, where C is a small constant. This relationship is commonly known as the birthday paradox.)

Chapter 6

6.1 **a)** We know that $d \cdot e = 1 \bmod \phi(n)$ i.e., $d \cdot 379 = 1 \bmod 3999996$.

Euclid's algorithm (Read down)	**Bezout's identity** (Read up)
$3999996 = 10554 \cdot 379 + 30$	$= 139 \cdot (3999996 - 10554 \cdot 379) - 11 \cdot 379 = 139 \cdot 3999996 - 1467017 \cdot 379$
$379 = 12 \cdot 30 + 19$	$= 7 \cdot 30 - 11 \cdot (379 - 12 \cdot 30) = 139 \cdot 30 - 11 \cdot 379$
$30 = 1 \cdot 19 + 11$	$= 7 \cdot (30 - 1 \cdot 19) - 4 \cdot 19 = 7 \cdot 30 - 11 \cdot 19$
$19 = 1 \cdot 11 + 8$	$= 3 \cdot 11 - 4 \cdot (19 - 1 \cdot 11) = 7 \cdot 11 - 4 \cdot 19$
$11 = 1 \cdot 8 + 3$	$= 3 \cdot (11 - 1 \cdot 8) - 1 \cdot 8 = 3 \cdot 11 - 4 \cdot 8$
$8 = 2 \cdot 3 + 2$	$= 3 - 1 \cdot (8 - 2 \cdot 3) = 3 \cdot 3 - 1 \cdot 8$
$3 = 1 \cdot 2 + 1$	$1 = 3 - 1 \cdot 2$
$2 = 2 \cdot 1 + 0$	

This gives $d = -1467017 = 2532979 \bmod \phi(n)$.

b) We use that $n = p \cdot q = 4003997$.

$$\begin{aligned} \phi(n) = &\quad (p-1)(q-1) = p \cdot q - p - q + 1 = n - p - q + 1 \\ 3999996 = &\quad 4003997 - p - q + 1 \Leftrightarrow \\ \Leftrightarrow p = &\quad 4002 - q \\ n = &\quad p \cdot q \end{aligned} \Rightarrow \quad (q - 2001)^2 = 4 = 2^2$$

We can choose $(p, q) = (1999, 2003)$ or $(p, q) = (2003, 1999)$.

6.2 If $p = 11$ and $q = 17$ we have $n = 187$ and $\phi(n) = (11-1)(17-1) = 160$. The system can be seen as RSA with $e = 3$. Euclid's algorithm gives $d = 107$.

a) We use the fact that $(R^3)^{107} = R \bmod 187$.

$$\begin{aligned} R_A = &\quad 104^{107} &&= 25 \bmod 187 \\ R_B = &\quad 58^{107} &&= 31 \bmod 187 \end{aligned}$$

This gives $R_A + R_B = 56$.

b) We have $R_A R_C = 122 - R_D = 122 - 49 = 73$. We know that $R_C = 160$ so

$$R_A = 73 \cdot 160^{-1}.$$

Euclid's algorithm gives that $160^{-1} = 90 \bmod 187$ so $R_A = 25$. From a) we have the sum $R_A + R_B = 56$ which gives $R_B = 31$.

6.3 The attacker can create the ciphertext $c' = 2^e c \bmod n$ and ask for the decryption of c'. He will then get the plaintext m' and

$$m' = (c')^d \bmod n = (2^e c)^d \bmod n = (2^{ed} \bmod n)(c^d \bmod n) = 2m \bmod n.$$

Thus, he can recover the message m by computing

$$m = \frac{m'}{2} = m' \cdot 2^{-1} \bmod n.$$

Since n is odd, 2 will always have an inverse in $\mathbb{Z}_n$.

6.4 **a)** With $p = 23$ and $q = 29$ we have $n = 667$ and $\phi(n) = (p-1)(q-1) = 616$. We want to find $d = e^{-1} = 3^{-1} \bmod 616$.

$$616 = 3 \cdot 205 + 1 \Rightarrow 616 - 3 \cdot 205 = 1 \bmod 616 \Rightarrow 3^{-1} = -205 = 411 \bmod 616.$$

Thus, $d = 411$.

b) We want to find $m = c^d \bmod n = 2^{411} \bmod 667$. We can write 411 in binary as 110011011. Hence

$$2^{411} = 2^{256} \cdot 2^{128} \cdot 2^{16} \cdot 2^8 \cdot 2^2 \cdot 2^1.$$

We can write a table for the powers mod 667. (shown to the right) Hence,

$$m = 2^{411} = 422 \cdot 634 \cdot 170 \cdot 256 \cdot 4 \cdot 2 = 200 \bmod 667.$$

2^1	2 mod 667
2^2	4 mod 667
2^4	16 mod 667
2^8	256 mod 667
2^{16}	170 mod 667
2^{32}	219 mod 667
2^{64}	604 mod 667
2^{128}	634 mod 667
2^{256}	422 mod 667

c) Using the chinese remainder theorem and the fact that $a^{p-1} = 1 \bmod p$ when p is prime, we can write

$$\begin{aligned} m_1 &= 2^{411} \bmod 23 = 2^{22 \cdot 18 + 15} \bmod 23 = 2^{15} \bmod 23 = 16 \bmod 23 \\ m_2 &= 2^{411} \bmod 29 = 2^{28 \cdot 14 + 19} \bmod 29 = 2^{19} \bmod 29 = 26 \bmod 29 \end{aligned}$$

Using the chinese remainder theorem

$$m = m_1 N_1 M_1 + m_2 N_2 M_2 \bmod n$$

with parameters $n = 667$, $n_1 = 23$, $n_2 = 29$, $N_1 = n/n_1 = 29$, $N_2 = n/n_2 = 23$, $M_1 = 29^{-1} \bmod 23 = 6^{-1} \bmod 23 = 4 \bmod 23$ and $M_2 = 23^{-1} \bmod 29 = (-6)^{-1} \bmod 29 = -5 = 24 \bmod 29$ we get

$$m = 16 \cdot 4 \cdot 29 + 26 \cdot 23 \cdot 24 = 200 \bmod 667.$$