QUESTION	
1	One time pad is an simple crytosystem which has perfect secrecy. However, cryptographysecurityprivacy people will tell you that it is vulnerable to a Known-Plaintext attack (KPA): 1010001111000011000000101110000111100000111000001100000000100001000000111100000110100011111000101010000110000000000000111000001011100000111000000000001001000010101000010110001101000011111000110110000011000000100
2	We received this blank image. Can you find the flag?
3	We received two images and were told to "spot the difference". A hint was also given, "The DIFFERENCE is a tool".
4	This executable computes a deterministic function of an input. What will be the result of this function, in hexadecimal, for the input 0xdead?
5	Alice and Bob like the prime number p =773 and the primitive root g=2. They plan to use it to perform a Diffie-Hellman key exchange. Alice has chosen her secret key a=313, while Bob has chosen the number b = 657. We will have a talk with them later about choosing more appropriately sized numbers for security, but in the meantime calculate their shared secret for them.

6	What kind of encryption preserves the properties described in the following: that applying the encryption algorithm to the product of m1 and m2 produces the same result as the product of c1 and c2. Where m indicates a message and c indicates a ciphertext. Additionally, the encyption of m1 + m2 produces the sum of c1 and c2.
7	The Diffie-Hellman key exchange relies on the hardness of what mathematical problem:
8	Groups are one of the mathematical structures that are used in cryptography. There is a type of group where applying the group operation to two elements of the group is independent of the order. What kind of group is this?
9	What is the effective keysize of the DES cipher in bits?
10	Consider a Shamir (3, 5)-threshold scheme with 17 = # Z_17 (integers modulus 17). Alice, Bob, and Carol pool their shares to produce the following equations. (x_0 +x_1 + x_2 = 8), (x_0 +2x_1 +9x_2 = 10), (x_0 +5x_1 + 8x_2 = 11). Determine the key.
11	We received a message and know there is a flag hidden in it somewhere; please find it for us. This was the message received: "46 4C 41 47 7B 77 30 6D 33 4E 30 66 42 6C 33 74 63 68 6C 33 59 7D".

<table>
<tr><td>12</td><td>We received a message but can't decipher it. Can you retrieve the hidden flag? This was the message received, "01000110 01001100 01000001 01000111 01111011 00110001 00111001 00110001 00110010 01001010 01110101 01101110 01100101 00110010 00110011 01111101".</td></tr>
<tr><td>13</td><td>Please help us find the flag in the message! ". /`A/\/\ 7nE-.e=|=|1)| A n1 29N1H7 @ <|OOL oO|_ =|1 })|N1=|o7/`5aE51{9Alh>| hE7 2E|/\|17E|/\|o5"</td></tr>
<tr><td>14</td><td>We keep receiving mysterious messages containing flags. The latest is: "..-. .-.. .- --. # -- .. .-.. - --- -. -.- . -.-- -. . ... #".</td></tr>
<tr><td>15</td><td>It is well-known that musicians were fans of steganography and they used it in a number of different ways. This flag will be BACH. (Don't write natural symbols or use punctuation.)</td></tr>
<tr><td>16</td><td>What four pair hex sequence do PDF files start with?</td></tr>
<tr><td>17</td><td>What does CISSP stand for?</td></tr>
<tr><td>18</td><td>What is the familiar name for CVE-2014-0160?</td></tr>
<tr><td>19</td><td>An assembly code implementation of an encryption algorithm uses different instructions, depending on the value of a bit. These instructions have different power consumptions. What kind of attack can an attacker execute on such a system?</td></tr>
<tr><td>20</td><td>According to Shodan.io, which country has the highest number of vulnerable Minecraft servers?</td></tr>
</table>

21	What is the IP address on the line "the. thoroughbred.of.sin" when you run a traceroute for "bad.horse"?
22	What string do you pass to the chmod command to make a file executable by you and not readable or writeable or executable by any other user?
23	What is the Answer to the Ultimate Question of Life, the Universe, and Everything?
24	Hack the ______!
25	In Futurama, what is Fry's debit card PIN?
26	To play media and web content, Firefox generates a new child process. This stops the executable web content from obtaining all the privileges of the original Firefox process. What is this technique called?
27	When is xkcd.com's certificate valid until (YYYYMMDD)?
28	What version of Apache runs on the CrySP server? (https://www.crysp.uwaterloo.ca)
29	Eve wants to spoof packets directed to Alice's device on her local network, which has a different MAC and IP address. She enables port forwarding and reroutes her IP tables to handle incoming traffic. Now, she needs to dupe Alice's device into believing that her device is the network gateway. What is a command to do this?