INSTRUCTOR VERSION WITH ANSWERS & FEEDBACK SHOWN

May 15, 2017

Encryption: Security Through Mathematics

Center for Science of Information, A National Science Foundation Science & Technology Center `http://soihub.org`

Questions on *Encryption: Security Through Mathematics*

1. Which of the following is/are true:
   - ○ A continuous memoryless channel takes continuous inputs and continuous outputs, and is indexed by a continuous time index.
   - ○ C(P) is non-decreasing, concave and left-continuous for any real function $\kappa(x)$. ✓
   - ○ $\frac{1}{n}\sum_{i=1}^{n}\kappa(x_i) \leq P$ in the definition of (κ, P) implies that the input distribution here is restricted to discrete random variable X.
2. Which of the following about the converse proof is/are true:
   - ○ $h(\mathbf{Y}|\mathbf{X}) = \sum_{i=1}^{n} h(Y_i|X_i)$ due to the retention property of the channel.
   - ○ We have to show $I(X_i; Y_i) \leq C(P)$ before we show $\sum_{i=1}^{n} I(X_i; Y_i) \leq nC(P)$.
   - ○ The concavity of mutual information $\frac{1}{n}\sum_{i=1}^{n} I(X_i; Y_i) \leq I(X; Y)$ is based on $X \sim \frac{1}{n}\sum_{i=1}^{n} F_i(x)$. ✓
   - ○ The concavity of mutual information $\frac{1}{n}\sum_{i=1}^{n} I(X_i; Y_i) \leq I(X; Y)$ is based on $X \sim \frac{1}{n}\sum_{i=1}^{n} X_i$.
3. Is this true (Y/N): It is difficult to formulate the notion of jointly typicality as in discrete case because the input distribution F(x) may not have a pdf.
   - ○ Y ✓
   - ○ N
4. Is this true (Y/N): The random coding scheme requires the sequence length n to be sufficiently large.
   - ○ Y ✓
   - ○ N
5. Is this true (Y/N): In the random coding scheme, there is zero probability for a codeword to violate the constraint.
   - ○ Y ✓
   - ○ N

6. Which of the following is/are true:
   - ○ The signal-to-noise ratio P/N of a memoryless Gaussian channel has to be greater than 1 so that its capacity is positive.
   - ○ If there is an input power constraint, we can transmit information through a memoryless Gaussian channel reliably at any finite rate.
   - ○ $h(Y|X) = h(Z|X)$ for Y = X+Z because conditioning on X, Y and Z determine each other. Therefore, given X, Y and Z carries the same amount of information.
   - ○ $h(Z|X) = h(Z)$ because Z is independent of X. ✓

7. The capacity of the parallel Gaussian channels system is attained when:
   - ○ The inputs are dependent of each other.
   - ○ The inputs are Gaussian. ✓
   - ○ The output powers are allocated according to water-filling.
   - ○ Every channel is used.

8. Which of the following is/are true:
   - ○ The equivalent system is a system of Gaussian channels with decorrelated noise vector. ✓
   - ○ The capacity of a system of correlated Gaussian channels is attained when the inputs are mutually independent.
   - ○ Multiplying an input vector **X** by Q and then transmitting it through the correlated Gaussian channels produce the same output as transmitting it through the equivalent channel.

9. Which of the following is true:
   - ○ The orthonormal basis of signals bandlimited to $0, W$ is given by $\psi_i(t) = \sqrt{2W}\text{sinc}(2Wt - i), i \in (-W, W)$.
   - ○ The orthonormal basis of signals bandlimited to $0, W$ is given by $\psi_i(t) = \frac{1}{\sqrt{2W}}\text{sinc}(2Wt - i), i \in (-\infty, \infty)$.
   - ○ $\psi_i(t) i \in (-\infty, \infty)$ form an orthonormal because each $\psi_i(t)$ has energy 1 and $\psi_i(t), \psi_j(t)$ has cross-correlation function 0 at $\tau = 0$ for distinct i, j. ✓

10. Which of the following is/are true:
    - ○ The bandlimited white Gaussian channel is equivalent to a system of correlated Gaussian channels.
    - ○ The noise power of the corresponding memoryless Gaussian channel is N_0 W.
    - ○ $Z(\frac{i}{2W}) i \in (-\infty, \infty)$, i.e. the unfiltered $Z(t)$ with $t = \frac{i}{2W}$, are i.i.d. Gaussian random variables with zero mean.
    - ○ If $X(t)$ has power constraint P, then X_i is constrained to $\frac{P}{2W}$. ✓

11. Capacity of the bandlimited colored Gaussian channel:
    - ○ $C(P) = \int_{-W}^{W} \log(1 + \frac{(-S_Z(f))^+}{S_Z(f)}) df$, where $\frac{1}{2}\int_{-W}^{W} (-S_Z(f))^+ df = P$.
    - ○ $C(P) = \frac{1}{2}\int_{-W}^{W} 1 + \frac{(-S_Z(f))^+}{S_Z(f)} df$, where $\int_{-W}^{W} \log(-S_Z(f))^+ df = P$. ✓
    - ○ $C(P) = \frac{1}{2}\int_{-W}^{W} \log(1 + \frac{(-S_Z(f))^+}{S_Z(f)}) df$, where $\int_{-W}^{W} (-S_Z(f))^+ df = P$.

12. Which of the following is true:
    - ○ The zero-mean Gaussian noise has the largest differential entropy among all the additive noises with the same correlation matrix. ✓
    - ○ The diagonal elements of the correlation matrix after diagonalization specify the power of the individual noise variables.
    - ○ Data processing increases the information divergence between two random variables.

Vigenere Cipher

1. The Caesar cipher is a simplification of the Vigenere cipher, in which all characters are shifted by the same amount, the key letter. Use the Caesar cipher to encode the following message with the key letter "K":

   `Birds of a feather flock together.`

   Solution: Since K is the eleventh letter in the alphabet, all characters in the phrase are shifted 10 letters, which results in the phrase:

   `Lsbnc yp k pokdrob pvymu dyqodrob.`

2. Use the Vigenere cipher to encode the following message using the keyword "key":

   `The quick brown fox jumps over the lazy dog.`

   Solution: Since K is the eleventh letter in the alphabet, every third letter is shifted 10 letters starting with the first letter. Similarly, for E, every third letter is shifted 4 letters starting with the second letter. Finally, for Y, every third letter starting with the third letter is shifted 24 letters. Hence, the corresponding ciphertext is

   `Dlc aygmo zbsux jmh nswtq yzcb xfo pyjc byk.`

3. Suppose we wanted to crack the Vigenere cipher and we were given a long, encoded message M. Suppose a and b are two substrings in M which match. What are possibilities for the length of the key? What can we do once we know the length of the key?

   Solution: Let n be the number of characters between a and b in M. Then the length of the key divides n with non-negligible probability. Hence, if g is a number that divides n, split M into g groups, by every gth character, and perform frequency analysis. This form of attack is known as the Kasiski examination.

Playfair Cipher

One way to develop a Playfair square is to use a five-by-five square and omit the letter J. That is, during encoding and decoding, $I = J$. Moreover, the first row(s) will be the keywords with redundant letters omitted, and then the remaining squares are filled in with the alphabet, in order. For example, the Playfair square for keyword "CRYPTOGRAPHY" is:

C	R	Y	P	T
O	G	A	H	B
D	E	F	I	K
L	M	N	Q	S
U	V	W	X	Z

4. What is the Playfair square for the keyword "BOILERMAKER" look like?

   Solution:

B	O	I	L	E
R	M	A	K	C
D	F	G	H	N
P	Q	S	T	U
V	W	X	Y	Z

5. What is the encryption, with the previous Playfair square for key "BOILERMAKER", for the following phrase:

   ```
   No free lunch
   ```

   Solution: First, we split the phrase into groups of two letters, adding Z to the end.

   ```
   No fr ex el un ch
   ```

   Next, use the rules of Playfair to encrypt each group of two letters, to obtain the encrypted message:

   ```
   Fe dm iz be zu kn
   ```

Strengthening the Vigenere Cipher

Use the one-time pad "A penny saved is a penny earned" to encrypt the following messages:

6. `Practice makes perfect`

   Solution:

   ```
   Pgepggue henmk ptvsrax
   ```

7. `Just use frequency analysis!`

   Solution:

   ```
   Jjwg hqw fmitcwnrc naypyjvw!
   ```

Cryptography and Entropy Part 1

8. Is the Caesar Cipher perfectly secure?

   Solution: Of course not, we already know how to decrypt it! Moreover, if two characters in the ciphertext are the same, then the two corresponding characters in the plaintext must be the same.

9. Intuitively, is the Vigenere Cipher perfectly secure?

   Solution: Intuitively, the Vigenere Cipher is not perfectly secure, since we can decrypt it!

10. Even though using a one-time pad is perfectly secure, why might using the same one-time pad repeatedly be insecure?

    Solution: Using a one-time pad repeatedly reveals information about the characters in the same positions. For example, if two ciphertexts began with the same letter, then their plaintexts must begin with the same letter too.

Cryptography and Entropy Part 2

11. A scheme that is perfectly secure has
$$H(M|C) = H(M).$$
What relationship holds for all encryption schemes?

Solution: Encryption schemes can only give information about the original message, which lowers the entropy, so
$$H(M|C) \leq H(M).$$

12. If an encryption scheme is perfectly secure, how do the number of keys and the number of possible messages relate? What does this say about perfect security in practice?

Solution: Given a ciphertext C and encryption scheme f, for each key k, there is at most one message M such that $f_k(M) = C$. Hence, the number of (k, M) pairs for which $f_k(M) = C$ is at most the number of keys. If this value is less than the number of possible messages, then there exists message M' such that $f_{k'}(M') \neq C$ for all keys k', which changes the distribution of the possible messages. Thus, a perfectly secure encryption scheme must have number of keys at least the number of possible messages. In practice, perfect security is very difficult to achieve because of the sheer number of possible messages.

13. In the previous section, we determined that intuitively, the Vigenere Cipher is not perfectly secure. Now prove mathematically, that both the Vigenere Cipher and the Playfair Cipher are not perfectly secure.

Solution: Because the keys of the Vigenere and Playfair Ciphers are shorter than most messages, the encryption schemes cannot be perfectly secure.

Cryptography and Entropy Part 3

14. Compute the unicity point of the Vigenere Cipher for the English language using keywords of length 3, and only using frequency analysis. ($H = 4.2$)

Solution: The unicity point is
$$\frac{\log_2(|K|)}{\log_2(|C|) - H} = \frac{\log_2(26^3)}{\log_2(26) - 4.2} \approx 28.178$$

15. How do the unicity points relate for the Caesar Cipher and the Vigenere Cipher? Why is this the case?

Solution: The unicity point of the Caesar cipher is lower than the unicity point of the Vigenere Cipher, because the number of possible keys for the Vigenere Cipher is much greater than the number of possible keys for the Caesar cipher.

One-Way Functions

16. Define a one-way function. Why might it be useful for encryption?

Solution: A one-way function is a function that is easy to compute given the inputs, but difficult to calculate the inputs given the output. That is, the function is difficult to invert.

17. Determine a method which uses multiplication as a one-way function.

Solution: One way is to determine two large primes p and q. Then pq is easy to compute, but factoring pq is more difficult.

Discrete Logarithms, Diffie-Hellman Key Exchange

18. Compute the product of the two primes, $3253 \cdot 3559$. Factor the number 1927. Which problem was more difficult?

Solution: By computation,

$$3253 \cdot 3559 = 11577427.$$

By trial and error,

$$1927 = 41 \cdot 47.$$

19. Compute $5^{32} \pmod{33}$. Determine p for which

$$14^p \equiv 5 \pmod{17}.$$

Which problem was more difficult?

Solution: By Fermat's Little Theorem,

$$5^{32} \equiv 25^{16} \pmod{33} \equiv 31^8 \pmod{33} \equiv 4^4 \pmod{33} \equiv 25 \pmod{33}.$$

By trial and error,

$$14^{13} \equiv 5 \pmod{17}.$$

20. What is the purpose of the Diffie-Hellman Key Exchange? That is, what does the Diffie-Hellman Key Exchange accomplish?

Solution: The purpose of the Diffie-Hellman Key Exchange is for two parties to agree on a password over a public channel, one prone to eavesdropping. However, both parties will obtain the same password, while the eavesdropper is unable to arrive at the same conclusion.

21. Derive a key-exchange system for three parties, in a similar way to the Diffie-Hellman exchange.

Solution: Given keys a, b, c for parties A, B, C and prime p and agreed values g, p, A sends g^a to B, who then sends g^b and g^{ab} to C. C then sends g^c and g^{bc} to A. A sends g^{ac} to B. Then all three parties can compute mutual password g^{abc}, but an eavesdropper cannot.

The RSA Algorithm Under the Hood Part 1: Prime Numbers, Euclidean Algorithm

22. In the corresponding lecture, it was proven that there are infinitely many prime numbers. In the same idea of the proof, given a positive integer n, determine n consecutive composite numbers.

Solution: Consider the n integers

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n, (n+1)! + (n+1).$$

Note that the kth integer in the list is divisible by $(k+1)$, so the n consecutive integers are all composite.

The RSA Algorithm Under the Hood Part 2: Prime Numbers, Euclidean Algorithm

23. Use the Euclidean Algorithm to find the greatest common divisor of 3924 and 56232

    Solution: The greatest common divisor of 3924 and 56232 is 36.

24. Use the Euclidean Algorithm to determine whether 724 and 813 are relatively prime.

    Solution:

$$\begin{aligned} 813 &= 724 \cdot 1 + 89 \\ 724 &= 89 \cdot 8 + 12 \\ 89 &= 12 \cdot 7 + 5 \\ 12 &= 5 \cdot 2 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Hence, the greatest common divisor of 724 and 813 is 1, so the numbers are relatively prime.

The RSA Algorithm Under the Hood Part 3: Greatest Common Divisor and Fermat's Little Theorem

25. Use the Euclidean Algorithm to determine a and b such that

$$2232a + 1645b = 1.$$

Solution:

$$\begin{aligned} 2232 &= 1645 \cdot 1 + 587 \\ 1645 &= 587 \cdot 2 + 471 \\ 587 &= 471 \cdot 1 + 116 \\ 471 &= 116 \cdot 4 + 7 \\ 116 &= 7 \cdot 16 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \end{aligned}$$

Then we have

$$\begin{aligned}
1 &= 4+3\cdot(-1)\\
&= 4+(7-4)(-1)\\
&= 7\cdot(-1)+4\cdot 2\\
&= 7\cdot(-1)+(116-7\cdot 16)\cdot 2\\
&= 116\cdot 2+7\cdot(-33)\\
&= 116\cdot 2+(471-116\cdot 4)(-33)\\
&= 471\cdot(-33)+116\cdot 134\\
&= 471\cdot(-33)+(587-471)(134)\\
&= 587\cdot 134+471\cdot(-167)\\
&= 587\cdot 134+(1645-587\cdot 2)(-167)\\
&= 1645\cdot(-167)+587\cdot(468)\\
&= 1645\cdot(-167)+(2232-1645)(468)\\
&= 2232\cdot 468+1645\cdot(-635)
\end{aligned}$$

Hence, $a = 468$ and $b = -635$.

26. Use the Euclidean Algorithm to determine the greatest common divisor, g, of 31824 and 864, and a and b such that

$$31824a + 864b = g.$$

Solution:

$$\begin{aligned}
31824 &= 864\cdot 36+720\\
864 &= 720\cdot 1+144\\
720 &= 144\cdot 5
\end{aligned}$$

Thus, the greatest common divisor is $g = 144$. Moreover,

$$\begin{aligned}
144 &= 864\cdot 1+720\cdot(-1)\\
&= 864\cdot 1+(31824-864\cdot 36)(-1)\\
&= 31824\cdot(-1)+864\cdot 37
\end{aligned}$$

Hence, $a = -1$ and $b = 37$.

The RSA Algorithm Under the Hood Part 4

27. Fermat's Little Theorem states that for p prime and a relatively prime to p,

$$a^p \equiv a \pmod{p}.$$

Find a counterexample if p can be any integer and a is not relatively prime to p.

Solution: One simple example is $a = 2$ and $p = 16$, then

$$a^p = 2^{16} \equiv 0 \pmod{16} \neq a \pmod{p}.$$

28. The RSA encryption algorithm requires finding b, given an integer a, such that

$$ab \equiv 1 \pmod{m},$$

for some modulo m. How can this be achieved?

Solution: Since a and m must be relatively prime, this can be achieved using the Euclidean Algorithm, as in the previous lectures.

29. Given $a = 17$ and $m = 329$, find b such that

$$ab \equiv 1 \pmod{m}.$$

Solution: Using the Euclidean Algorithm,

$$\begin{aligned} 329 &= 17 \cdot 19 + 6 \\ 17 &= 6 \cdot 2 + 5 \\ 6 &= 5 \cdot 1 + 1 \end{aligned}$$

Hence,

$$\begin{aligned} 1 &= 6 \cdot 1 + 5 \cdot (-1) \\ &= 6 \cdot 1 + (17 - 6 \cdot 2)(-1) \\ &= 17 \cdot (-1) + 6 \cdot 3 \\ &= 17 \cdot (-1) + (329 - 17 \cdot 19)(3) \\ &= 329 \cdot 3 + 17 \cdot (-4) \end{aligned}$$

so the inverse of 17 in modulo 329 is -4, which is just 325.

30. What type of encryption does RSA achieve? That is, what scenario is the RSA encryption algorithm useful?

Solution: RSA is an algorithm for public-key cryptography, which means public users can send encrypted messages to the original user of RSA, who can then decrypt the messages. The beauty is that there is no private channel, no secret sharing at all! There is only a public key which the original user publishes, and anyone can use to encrypt.

The RSA Algorithm Under the Hood Part 5

In the RSA encryption algorithm, p, q are primes such that $n = pq$ and a, b are integers such that

$$ab \equiv 1 \pmod{(p-1)(q-1)}.$$

31. Suppose Alice has knowledge of all the variables and wants to implement the algorithm. Which variables does she publish?

Solution: Alice publishes n and a.

32. Suppose Bob wants to encrypt message M and send it to Alice. What does he send?

Solution: Bob sends $M^a \pmod{n}$ back to Alice.

33. How does Alice decrypt the received message M'?

Solution: Alice decrypts by calculating $(M')^b$, which equates to

$$(M')^b \pmod{n} = (M^a)^b \pmod{n} = M^{ab} \pmod{n}.$$

Since $ab = 1 \pmod{\phi(n)}$, then $M^{ab} \equiv M \pmod{n}$.

34. Suppose an adversary intercepts message M'. What makes M' difficult to decrypt?

Solution: Since a is published, b must be difficult to compute. This is because $(p-1)(q-1)$ is not public knowledge. The primes p and q can only be computed by factoring the published value $n = pq$, but factoring is difficult.

The RSA Algorithm Under the Hood Part 6

35. Compute by hand $5^{82} \pmod{3123}$.

Solution: Via computation,

$$\begin{aligned}
5^1 &\equiv 5 \pmod{3123} \\
5^2 &\equiv 25 \pmod{3123} \\
5^4 &\equiv 625 \pmod{3123} \\
5^5 &\equiv 2 \pmod{3123} \\
5^{10} &\equiv 4 \pmod{3123} \\
5^{20} &\equiv 16 \pmod{3123} \\
5^{40} &\equiv 256 \pmod{3123} \\
5^{82} &\equiv 5^{40}5^{20}5^{10}5^5 5^4 5^2 5^1 \\
&\equiv 256 \cdot 16 \cdot 4 \cdot 2 \cdot 625 \cdot 25 \cdot 5 \\
&\equiv 256 \cdot 16 \cdot 625 \cdot 4 \cdot 25 \cdot 2 \cdot 5 \\
&\equiv 256 \cdot 10000 \cdot 100 \cdot 10 \\
&\equiv 25600000000 \pmod{3123} \\
&\equiv 1948 \pmod{3123}
\end{aligned}$$

Hence, the equivalence is $1948 \pmod{3123}$.