Written exam in TSIT03 Cryptology

14:00–18:00, 26 August 2017

Jan-Åke Larsson
Institutionen för Systemteknik,
Linköpings Universitet

Permitted equipment: General dictionaries between English and another language without personal notes. (Thus not specific scientific dictionaries with or without formulæ.)

Solutions: Solutions will be posted on the course home page after the exam.

Grading: Grade n requires at least $6n + 2$ points,
this translates to ECTS grade $20 - 2n$ (converted to hexadecimal)

Other information: Answers can be in English or Swedish

1. Historical ciphers

   (a) Decrypt the message below (hint: you have the key). (2p)

   3,3,1; 3,13,2; 1,1,3; 2,25,4; 2,4,5; 2,9,6; 1,5,3; 1,30,2; 1,11,1; 1,11,1; 3,2,6; 3,2,7; 2,25,1; 2,16,6; 3,2,8; 3,2,8; 2,16,6; 2,9,10; 2,9,8; 1,9,3; 1,1,5;

   (b) What is the key called using the course terminology? (1p)

   (c) Mention one weakness of the cipher (there are several). (1p)

   (d) Modern block ciphers have a mode of operation whose name alludes to the cipher above. What is it called? (1p)

   (e) Should the block-cipher mode in d) be used? Why? (2p)

2. Block ciphers

   (a) What block size does AES have? What is the recommended key length for AES? (2p)

   (b) AES uses calculation in the finite field GF(256) with the primitive polynomial $X^8 + X^4 + X^3 + X + 1$. Calculate $X^2 * (X^7 + X^6 + X^3 + X + 1)$ in the field. (1p)

   (c) Draw a diagram of Cipher Feedback mode. Give two good properties of the mode. (2p)

3. Information theory

   (a) Which are the most common and second-most common letter in English? (1p)

   (b) Why is the probability of the digram “TH” not equal to the probability of “T” multiplied with the probability of “H”? What is the probability-theory notion called that captures this property? (1p)

   (c) Give the formula for Shannon entropy in terms of a probability distribution $P(X = x)$. (1p)

   (d) The Shannon entropy connects with a particular kind of code that is adapted to the source distribution $P(X = x)$. What is the code called, and what is the key property of the code (in words, no mathematics is needed)? (2p)

4. Asymmetric ciphers

   (a) How do you choose the RSA parameters p, q, n, e, and d? (2p)

   (b) How is encryption and decryption done in RSA? (1p)

   (c) How is signing and verification done in RSA? (1p)

   (d) In RSA, what is a suitable number of bits for the public key n to give reasonable security? (1p)

   (e) What attack is possible if two public keys n_1 and n_2 happen to share one of the primes p? Is this a relevant question for existing implementations? (2p)

5. Elliptic curve cryptography

   (a) What is an elliptic curve, briefly? (1p)

   (b) What mathematical problem is the basis of security in Elliptic curve cryptography? (1p)

   (c) Describe Elliptic curve Diffie-Hellman key exchange. (2p)

   (d) If you want 128 “bits of security”, what key length do you need in ECC? How does this compare with RSA? (2p)

6. Divisibility in modular arithmetic

   (a) When is division with a possible, mod N? (1p)

   (b) Write down Fermat’s little theorem. (2p)

   (c) Define Euler’s totient function $\phi(n)$. (2p)

7. Bitcoin

The Proof-of-Work problem commonly used in Bitcoin and other Blockchain systems has three properties:

i) it's difficult to find a solution

ii) once a solution is found, it is easy to verify as being correct

iii) independent of the global hashrate, a solution will only be found with a constant rate

(a) What cryptographic tool is used to give properties i) and ii)? (1p)

(b) Describe how to change the difficulty of the Proof-of-Work problem in the Bitcoin protocol. (2p)

(c) Is the solution to the Proof-of-Work problem unique? (1p)

(d) When is the difficulty of the problem adjusted in the protocol, and how does this ensure property iii)? (2p)

Solutions

1. Historical ciphers

   (a) Decrypt the message below (hint: you have the key). (2p)

   3,3,1; 3,13,2; 1,1,3; 2,25,4; 2,4,5; 2,9,6; 1,5,3; 1,30,2; 1,11,1; 1,11,1; 3,2,6; 3,2,7; 2,25,1; 2,16,6; 3,2,8; 3,2,8; 2,16,6; 2,9,10; 2,9,8; 1,9,3; 1,1,5;

   - “This is not too difficult”

   (b) What is the key called using the course terminology? (1p)

   - The “code book” is the exam itself.

   (c) Mention one weakness of the cipher (there are several). (1p)

   - For example, the difficulty to distribute the code book

   (d) Modern block ciphers have a mode of operation whose name alludes to the cipher above. What is it called? (1p)

   - Electronic Code Book, ECB.

   (e) Should the block-cipher mode in d) be used? Why? (2p)

   - No. Repeated cleartext leads to repeated ciphertext, and this is also the case when using a historical-cipher-style physical code book.

2. Block ciphers

   (a) What block size does AES have? What is the recommended key length for AES? (2p)

   - Block size is 128 bits, and the possible (and recommended) key sizes are 128, 192 and/or 256 bits

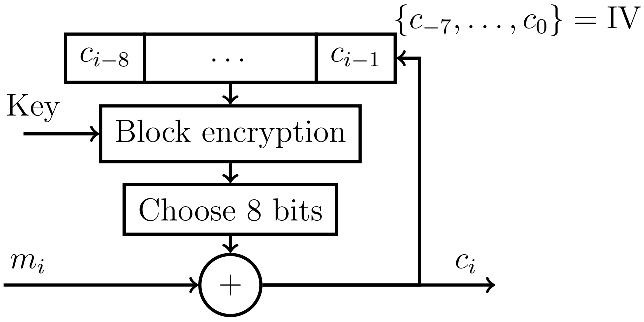
   (b) AES uses calculation in the finite field GF(256) with the primitive polynomial $X^8 + X^4 + X^3 + X + 1$. Calculate $X^2 * (X^7 + X^6 + X^3 + X + 1)$ in the field. (1p)

   - $X^2 * (X^7 + X^6 + X^3 + X^+1) = X^9 + X^8 + X^5 + X^3 + X^2$
     $= X * (X^8 + X^7 + X^4 + X^2 + X)$
     $= X * (X^8 + X^7 + X^4 + X^2 + X + X^8 + X^4 + X^3 + X + 1)$
     $= X * (X^7 + X^3 + X^2 + 1) = X^8 + X^4 + X^3 + X = 1$

   (c) Draw a diagram of Cipher Feedback mode. Give two good properties of the mode. (2p)

   - CFB can encrypt smaller message pieces than whole blocks

   - CFB can be used to test message integrity



3. Information theory

(a) Which are the most common and second-most common letter in English? (1p)

- “E” and “T”, in that order

(b) Why is the probability of the digram “TH” not equal to the probability of “T” multiplied with the probability of “H”? What is the probability-theory notion called that captures this property? (1p)

- The combination “TH” is much more common than one would think: on average, every fourth “H” is in “TH”. “Conditional probability,” or “dependent probability,” because the distribution of the following letter depends on which letter is first.

(c) Give the formula for Shannon entropy in terms of a probability distribution $P(X = x)$. (1p)

- $H(X) = -\sum_x P(X = x) \log_2 P(X = x)$

(d) The Shannon entropy connects with a particular kind of code that is adapted to the source distribution $P(X = x)$. What is the code called, and what is the key property of the code (in words, no mathematics is needed)? (2p)

- Huffman code
- Letters that have high probability are given short code words, and letters that have low probability are given long code words (the length is chosen to give as short average as possible)

4. Asymmetric ciphers

(a) How do you choose the RSA parameters p, q, n, e, and d? (2p)

- The parameters p and q are random very large primes, and $n = pq$. An important number here is $\varphi(n) = (p - 1)(q - 1)$, and e is chosen so that $\gcd(e, (p - 1)(q - 1)) = 1$. The final parameter d is chosen so that $ed = 1 \mod (p - 1)(q - 1)$.

(b) How is encryption and decryption done in RSA? (1p)

- With message m and cryptotext c, encryption and decryption are: $c = m^e \mod n$; $m = c^d \mod n$

(c) How is signing and verification done in RSA? (1p)

- With message m and signature s, signing and verification are: $s = m^d \mod n$, compare m and $s^e \mod n$.

(d) In RSA, what is a suitable number of bits for the public key n to give reasonable security? (1p)

- 3kbit of key is currently estimated to give 30 years protection

(e) What attack is possible if two public keys n_1 and n_2 happen to share one of the primes p? Is this a relevant question for existing implementations? (2p)

- If two public keys n_1 and n_2 happen to share one of the primes p, the extended Euclidean algorithm gives you $\gcd(n_1, n_2) = p$ immediately. This is relevant, because it seems some implementations choose between very few primes. Lenstra, Hughes et al. were able to factor 0.2% of a sample of public keys gathered from the Internet in early 2012.

5. Elliptic curve cryptography

   (a) What is an elliptic curve, briefly? (1p)

   - An elliptic curve is the set of solutions to $y^2 = x^3 + bx + c$.

   (b) What mathematical problem is the basis of security in Elliptic curve cryptography? (1p)

   - The Elliptic Curve discrete logarithm: Given two points A and B on an elliptic curve, it is difficult (high complexity) to find a number k so that $B = kA = A + A + \ldots + A$.

   (c) Describe Elliptic curve Diffie-Hellman key exchange. (2p)

   - Choose an elliptic curve E mod a prime number p and a point α on the curve. Alice should randomly generate a secret integer a and make $a\alpha$ public (as a point on E). Likewise, Bob takes a secret random integer b and makes $b\alpha$ public. Both can now create $k = b(a\alpha) = a(b\alpha)$.

   (d) If you want 128 "bits of security", what key length do you need in ECC? How does this compare with RSA? (2p)

   - You need twice as many bits in the key, here 256 bits. This is much shorter than in RSA.

6. Divisibility in modular arithmetic

   (a) When is division with a possible, mod N? (1p)

   - When $\gcd(a, N) = 1$.

   (b) Write down Fermat's little theorem. (2p)

   - Theorem: If p is a prime and p does not divide a, then $a^{p-1} = 1 \bmod p$.

   (c) Define Euler's totient function $\phi(n)$. (2p)

   - Euler's totient function $\phi(n)$ is the number of integers $1 \leq x \leq n$ such that $\gcd(x, n) = 1$.

7. Bitcoin

   The Proof-of-Work problem commonly used in Bitcoin and other Blockchain systems has three properties:

   i) it's difficult to find a solution

   ii) once a solution is found, it is easy to verify as being correct

   iii) independent of the global hashrate, a solution will only be found with a constant rate

   (a) What cryptographic tool is used to give properties i) and ii)? (1p)

   - A weakly collision-free hash function

   (b) Describe how to change the difficulty of the Proof-of-Work problem in the Bitcoin protocol. (2p)

   - A solution is found if the output of the hash function is less than a threshold, so that it is "close enough" to 0, but not necessarily equal to 0. Changing the threshold changes the difficulty of the problem.

(c) Is the solution to the Proof-of-Work problem unique? (1p)

- No. For a hash function, many inputs map to the same output. In addition, the proof-of-work problem uses a threshold, as described above

(d) When is the difficulty of the problem adjusted in the protocol, and how does this ensure property iii)? (2p)

- If the rate of found solutions is too large, the threshold T is decreased, making the problem more difficult. If the rate is too low, T is increased, making the problem easier. This is used to ensure that the rate of finding solution is independent of the global hashrate.