Written exam in TSIT03 Cryptology

14:00–18:00, 5 January 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

s	v	e	r	i
g	a	b	c	d
f	h	k	l	m
n	o	p	q	t
u	w	x	y	z

   (a) The above table can be used in one historical cipher mentioned in the course. What is it called? (1p)

   (b) What is the key in this case? (1p)

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

   (d) What is the main reason this cipher was created, how does it increase security compared to the other ciphers of the time? (1p)

   (e) The property used in d) is still an important property of modern ciphers, but has evolved. How? Give an example. (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)

   (d) What is the Horton principle (according to Bruce Schneier)? (1p)

3. Diffie-Hellman key exchange

   (a) For D-H key exchange in modular arithmetic, what kind of values are the secret parameters? What are the shared public parameters? How are the personal public parameters calculated from the secret and the general parameters? How is the shared key calculated? (3p)

   (b) Answer the same questions for D-H key exchange using elliptic curves. (3p)

4. Hash functions

   (a) What standard hash function was the result of a competition, and what was the name of the contribution that won? (2p)

   (b) How does an iterative hash function work (you do not need to protect against length extension)? Why is this construction used? (2p)

   (c) You are given a good cryptographic hash function h that you want to use as basis for a stream cipher. How do you implement such a cipher (draw a diagram, and specify input parameters)? (2p)

5. Secret sharing

   The owner of company X normally handles the combination of the company safe himself, but in case he cannot come to work, any two out of the six employees should be able to open the safe, if they cooperate. The owner regularly changes the combination to the safe and then of course the employees should get new shares. Suppose that the combination is changed to 4237.

   (a) Give a suggestion for a possible value for each of the six shares and describe how two shares are used to retrieve the correct combination. (2p)

   (b) How does he need to change his system if instead any three out of the six employees should be able to open the safe? (2p)

6. Discrete log one-way functions

   (a) Name one cryptographic system where the security depends on the hardness of the Discrete log problem (1p)

   (b) In "Discrete log systems" one public parameter is a prime number p. What is the currently recommended length of p? (1p)

   (c) Under the assumption that one particular length of p is appropriate for several users, give two arguments why it is a good idea to use the same p. (1p)

   (d) Under the assumption that one particular length of p is appropriate for several users, give one argument why it is NOT a good idea to use the same p. (1p)

   (e) Do current implementations follow c) or d), and is this a good idea? Why? (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

s	v	e	r	i
g	a	b	c	d
f	h	k	l	m
n	o	p	q	t
u	w	x	y	z

   (a) The above table can be used in one historical cipher mentioned in the course. What is it called? (1p)

   - "Playfair"

   (b) What is the key in this case? (1p)

   - The word "keyword"

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

   - For example, the final part of the table is predictable.

   (d) What is the main reason this cipher was created, how does it increase security compared to the other ciphers of the time? (1p)

   - It uses pairs of letters as a basic unit (digrams). This makes statistical analysis harder, than when using single letters.

   (e) The property used in d) is still an important property of modern ciphers, but has evolved. How? Give an example. (2p)

   - The block length of modern block ciphers is chosen to prohibit statistical analysis even with computers, AES for example has a block length of 128 bits.

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

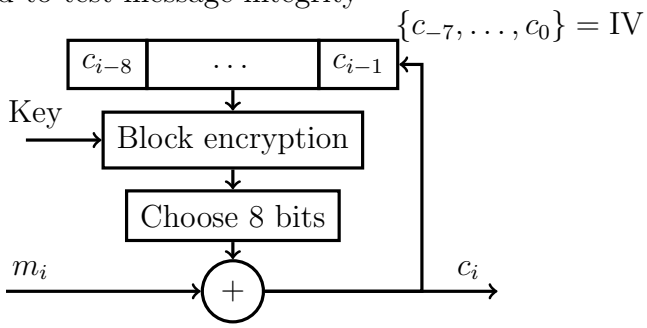
   (b) AES uses calculation in the finite field GF(256) with the primitive polynomial $X^8 + X^4 + X^3 + X + 1$. Calculate $X^2 * (X^7 + X^6 + X^3 + X + 1)$ in the field. (1p)

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

   (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



(d) What is the Horton principle (according to Bruce Schneier)? (1p)

- Authenticate what is ment, not what is being said

3. Diffie-Hellman key exchange

(a) For D-H key exchange in modular arithmetic, what kind of values are the secret parameters? What are the shared public parameters? How are the personal public parameters calculated from the secret and the general parameters? How is the shared key calculated? (3p)

- The public parameters are a prime p and a primitive root α mod p. Alice's secret parameter is a random integer a, while Bob's secret parameter is a random integer b. Alice makes α^a mod p public, while Bob makes α^b mod p public. Both can now create the shared key $k = (\alpha^a)^b = (\alpha^b)^a$ mod p

(b) Answer the same questions for D-H key exchange using elliptic curves. (3p)

- The public parameters are a prime p, an elliptic curve E and a point α on E. Alice's secret parameter is a random integer a, while Bob's secret parameter is a random integer b. Alice makes $a\alpha$ public, while Bob makes $b\alpha$ public. Both can now create the shared key $k = b(a\alpha) = a(b\alpha)$, note that this is a point on E.

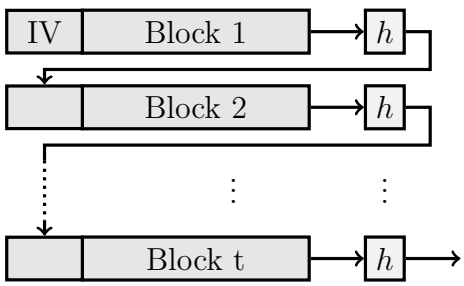
4. Hash functions

(a) What standard hash function was the result of a competition, and what was the name of the contribution that won? (2p)

- The SHA3 competition, and the winner was a contribution called Keccak.

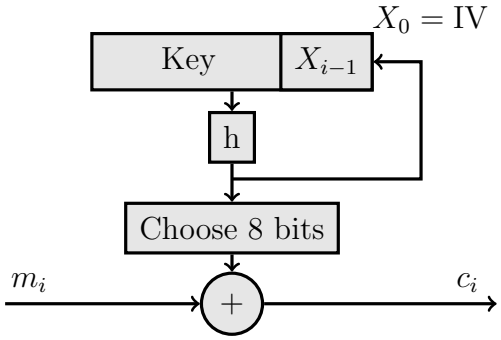
(b) How does an iterative hash function work (you do not need to protect against length extension)? Why is this construction used? (2p)

- The construction is used if one wants to hash arbitrary sized inputs using a hash function that takes a fixed size input.



(c) You are given a good cryptographic hash function h that you want to use as basis for a stream cipher. How do you implement such a cipher (draw a diagram, and specify input parameters)? (2p)

- A stream cipher, similar to OFB of a block crypto:



This is a symmetric key system. The key should be secret, while the IV can be sent with the message, but should be chosen at random.

5. Secret sharing

The owner of company X normally handles the combination of the company safe himself, but in case he cannot come to work, any two out of the six employees should be able to open the safe, if they cooperate. The owner regularly changes the combination to the safe and then of course the employees should get new shares. Suppose that the combination is changed to 4237.

(a) Give a suggestion for a possible value for each of the six shares and describe how two shares are used to retrieve the correct combination. (2p)

- Create any line $y = kx + 4237$. Then take six different random values for $x \neq 0$, find y for these and use these pairs as the shares. Any pair of employees can now reconstruct the line and find the value for $x = 0$.

(b) How does he need to change his system if instead any three out of the six employees should be able to open the safe? (2p)

- Create any line $y = ax^2 + bx + 4237$. Then take six different random values for $x \neq 0$, find y for these and use these pairs as the shares. Any triple of employees can now reconstruct the line and find the value for $x = 0$.

6. Discrete log one-way functions

(a) Name one cryptographic system where the security depends on the hardness of the Discrete log problem (1p)

- Diffie-Hellmann, ElGamal

(b) In "Discrete log systems" one public parameter is a prime number p. What is the currently recommended length of p? (1p)

- 3 kbit is the current recommendation for ∼30 years security.

(c) Under the assumption that one particular length of p is appropriate for several users, give two arguments why it is a good idea to use the same p. (1p)

- They can use the same secret key in several connections, and
- They do not need to negotiate which prime number p to use

(d) Under the assumption that one particular length of p is appropriate for several users, give one argument why it is NOT a good idea to use the same p. (1p)

- If many users use the same p it may suddenly be worth the effort to compute the discrete log for that p.

(e) Do current implementations follow c) or d), and is this a good idea? Why? (2p)

- They use the same p (at a given security), and no, this is not a good idea, the rumor is that NSA has the discrete log function for one of the supposedly secure ps.

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.