SPCS Cryptography Class Lecture 3

June 23, 2015

Autokey cipher

The autokey cipher is very similar to Vigenere cipher, except that when the key runs out, we will use the original message as the key.

Example

Suppose we want to encrypt `meetatthefountain` with the key `kilt`. Then,

Plaintext	`meeta tthef ounta in`
Key	`kiltm eetat thefo un`
Ciphertext	`WMPMM XXAEY HBRYO CA`

How would Bob decipher the message?

Does Kaisiski's method still work for Eve?

Autokey cipher

- However, this is prone to another attack.
- The idea is to guess a word that appears in the plaintext and use that to string along the rest of message.
- For example, THE is the most common trigram in English, so one can reasonably guess that THE appears somewhere in the message, thus is part of the key somewhere.

Autokey cipher

Example

Let us try to decipher the ciphertext we just had.

`WMPMM XXAEY HBRYO CA`

Assume that `the` appears somewhere in the plaintext. We can try all the possibilities fairly quickly, by assuming the key is

- THETHETHE (1 mod 3 case), or
- ·THETHETHE (2 mod 3 case), or
- ··THETHETHE (0 mod 3 case)

Autokey cipher

(1 mod 3 case):

Ciphertext	WMP MMX XAE YHB RYO CA
Key	the the the the the ..
Plaintext	dfl tft eta fax yrk ..

(2 mod 3 case):

Ciphertext	W MPM MXX AEY HBR YOC A
Key	. the the the the the .
Plaintext	. tii tqt hxu oun fhy .

(0 mod 3 case):

Ciphertext	WM PMM XXA EYH BRY OCA
Key	.. the the the the the
Plaintext	.. wfi eqw lrd iku vvw

Which plaintext looks plausible?

Autokey cipher

- Only eta, fax, oun look plausible.
- Since we also don't know the length of the key, so we have to guess a few possibilities.
- Suppose that Eve tries FAX.

Ciphertext	WMP MMX XAE YHB RYO CA
Key	... ... the ... ..
Plaintext	... ... fax ... ..

- Suppose she guesses the key length is 4.

Ciphertext	WMP MMX XAE YHB RYO CA
Key	... ..e qw. the .fa x.
Plaintext	... ..t he. fax .to f.

- While "tof" sounds plausible, "eqw" sounds unlikely. So Eve will probably try a new keylength, or try the other possibilities "eta" or "oun".

Autokey cipher

- The right answer in this case is OUN with key length of 4, giving

Ciphertext	`WMP MMX XAE YHB RYO CA`
Key	`k .lt m.e ta. the .ou n`
Plaintext	`m .et a.t he. oun .ai n`

- At this point, knowing the second letter of the key allows Eve to decrypt the message - she can try all the 26 possibilities here. If she chooses E, she would recover the message `meetatthefountain`.
- In practice, it is very difficult to break such a short autokey cipher. As we have seen, this is a general trend: longer messages are easier to break than shorter ones, because they have more structure to them.

Transposition ciphers

- We have looked at quite a few ciphers now: Caesar ciphers, shift ciphers, Vigenere ciphers, autokey cipher.
- They are all *substitution ciphers*.
- Another way of encrypting things is to directly permute the letters, without ever substituting them. These are *transposition ciphers*.
- Does frequency analysis help?

Columnar ciphers

Write horizontally, read vertically.

Example

Encrypt `defendtheeastwallofthecastle` with the key `german`.

Solution

G	E	R	M	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e		

Regular Columnar ciphers

Solution

For regular ones, we pad:

G	E	R	M	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e	x	x

Regular Columnar ciphers

Solution

Order the columns,

3	2	6	4	1	5
G	E	R	M	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e	x	x

Regular Columnar ciphers

Solution

Rearrange the columns,

1	2	3	4	5	6
A	E	G	M	N	R
n	e	d	e	d	f
a	h	t	e	s	e
l	w	t	l	o	a
c	t	f	e	a	h
x	t	s	e	x	l

Read vertically to get,

NALCXEHWTTDTTFSEELEEDSOAXFEAHL

How can Bob decipher the text?

Irregular Columnar ciphers

Solution

Irregular ones: Same thing without padding.

G	E	R	M	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e		

Irregular Columnar ciphers

Solution

Order the columns,

3	2	6	4	1	5
G	E	R	M	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e		

Solution

Rearrange the columns,

1	2	3	4	5	6
A	E	G	M	N	R
n	e	d	e	d	f
a	h	t	e	s	e
l	w	t	l	o	a
c	t	f	e	a	h
	t	s	e		l

Read vertically to get,

NALCEHWTTDTTFSEELEEDSOAFEAHL

How can Bob decipher the text?

Which one is harder, regular or irregular columnar ciphers?

Columnar ciphers

- What can Eve do?
- One can statistically check whether a passage looks like English by computer. Just keep trying various keylengths.
- Can do better if we add a diagram analysis, to see how likely two columns are next to each other.
- Can also decode it by hand (!), but of course would be slow. See `https://www.nsa.gov/public_info/_files/military_cryptanalysis/mil_crypt_iv.pdf`

Telling different ciphers apart

We have three categories of ciphers up to now,

- Transposition (Columnar, Rail-fence)
- Monoalphabetic Substitution (Caesar, Substitution, Affine)
- Polyalphabetic Substitution (Vigenere, Autokey)

How can we tell them apart?

Telling different ciphers apart

Some observations:

- Transposition ciphers do NOT change letter frequency at all.
- Monoalphabetic Substitution changes the order of letters, but not the PROFILE of letter frequency.
- Polyalphabetic Substitution changes the profile completely! It shouldn't feel like an English passage anymore statistically.

Friedman's index of coincidence

- Friedman's index of coincidence(IC) : detecting how likely two random letters coincide, with replacement.
- For random passage, IC is low. ($\frac{1}{26} \sim 0.0385$) (Vigenere is generally around 0.045)
- For English passage, IC is high. (around 0.07)

General strategy: to tell between transposition, monoalphabetic or polyalphabetic substitution,

- Check IC. High IC suggests transposition or monoalphabetic substitution. Low IC suggests polyalphabetic substitution.
- To distinguish transposition vs monoalphabetic substitution, check frequency.

Telling different ciphers apart

Example

The following is encrypted via columnar cipher, substitution cipher, or Vigenere cipher. Crack it.

```
VCKFZLRRIPPVVUQWRVRBPNXRBHMGTFPLCFTLRKYCNRFLLKSREBPNK
FROETRQALVDYKADGMTFIVWAHVESYSVNYZKVGRIUJPZFAJLBKEEJNH
TVFDJOCUQHMFEEAHVJRHFWRLKSKLBLNKJFLRGVNWEILNWOKZMUWFI
ILDZEQAAEKJFTYFSNHZKJLFKKFLDIZLREIJKVKZEEHTKYCLAIJDVR
JVTLRRCFVUIJYMTVIUHRUXGUNPNCHSCVWDHFYYKBVVLSOFBGUGGRJ
LWRJZBLCZCKIEKMAABZLNSFDCIYGVPJYKYCZTVRKWOLIGUGWIMTUE
UCYHVITPVZUFHIIXYCEKYCPMGICZSZFLAHRKFLRNYMSEYVYKWRJMU
FZIC
```

Telling different ciphers apart

(May or may not be) Useful tool:

- IC Check: `http://www.dcode.fr/index-coincidence`
- Letter Frequency: `https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html`
- Substitution cipher: `http://scottbryce.com/cryptograms/index.htm`
- Transposition cipher: `http://tholman.com/other/transposition/`

Introduction to Public Key Cryptography

- We have seen a few examples of ciphers now: substitution cipher, Vigenere cipher, autokey cipher etc.
- One thing in common: the same key is used for encryption and decryption. Such ciphers are called *symmetric ciphers*, and such encryption/decryption algorithm is called *symmetric-key algorithm.*

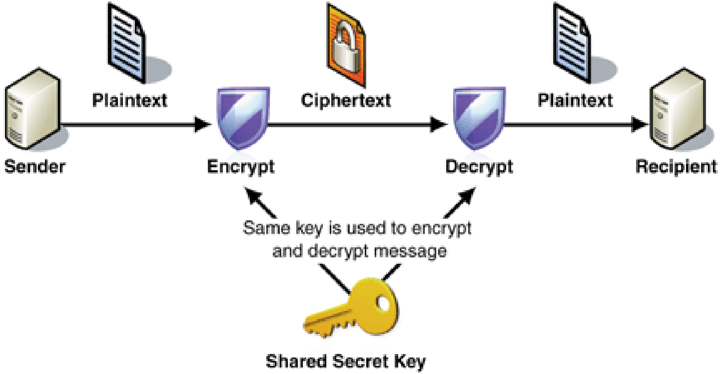

Image from `https://msdn.microsoft.com/en-us/library/ff650720.aspx`

Introduction to Public Key Cryptography

- A toy model of the situation is this: Alice and Bob have a safe and both has a key to the safe. When Alice wants to send Bob a message, she puts the message in the safe by opening the box (Encryption), close it, give it to Bob, who opens the box to retrieve the message. (Decryption)
- This requires Alice and Bob to meet in private beforehand to share the same key. What if they don't have such a chance?

Introduction to Public Key Cryptography

- William Jovens has an idea to solve this problem (Back in 1874!), but it was not implemented successfully until 1970s.
- The idea is simple: Alice and Bob does not need to share a safe - Bob would make a safe, as well as a secret key for the safe. The safe is designed in a way that even for someone who is free to look at and poke around with it, making a key that will open it is practically impossible.
- If Alice wants to send Bob a message, she only needs to put it in Bob's safe. (Encryption)
- If Bob wants to read the message, he opens the safe using his secret key (Decryption) and read the message.

Introduction to Public Key Cryptography

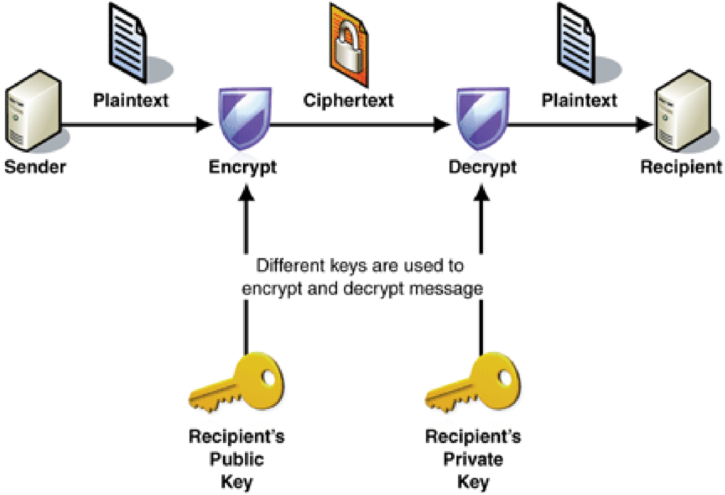

Image from https://msdn.microsoft.com/en-us/library/ff650720.aspx

Introduction to Public Key Cryptography

- Only problem is: how can Bob make such a safe?
- Also, if this method can be widely used, Kerckhoff's principle should be satisfied: every one knows how to make such a safe, but without the private key, only Bob can open it.
- One (philosophical) method: Use hard math problems.
- It turns out that there are math problems that are impossible to solve, without knowing the answer or just key to the answer. This is the basic idea of public-key cryptography.
- We will talk about Diffie-Hellman Problem and RSA Problem, the hard problems behind ElGamal Cryptosystem and the RSA system.

What happens in real life?

- Symmetric-key ciphers are still very important! They are easier to implement, and much faster to compute.
- Only problem - how to decide the shared key in the first place?
- We will talk about Diffie-Hellman Key Exchange. This is a process to let Alice and Bob get a shared key safely, even if they communicate in public channel.