Section 3 Lectures 17-19 – One-time pad

These notes are only supplementary material to the lectures

One time pad

I'll go through the principles of the one-time pad in the slides but this gives an example. This involves the two communicators Alice and Bob having an identical "pad" of random letters (the only two pads in existence), where they use each page once and then destroy it. Construction of these pads is not easy – I'll touch on some ideas why at the end and in the lecture.

We will label the letters by the numbers 0 to 25. 0 corresponds to "A", 1 corresponds to "B", 2 corresponds to "C", all the way up to 25 corresponding to "Z". So like this:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

We will consider letters in the message and the keyword as their numerical equivalent, and then doing modular arithmetic (mod 26)

Encrypting using the one-time pad

Having both got their copy of the pad, Alice and Bob start communicating. Alice wants to send the message "MEET ME AT THE CAFE TONIGHT" to Bob. We'll ignore spaces (it makes cracking much more difficult), so the text she wants to send is "MEETMEATTHECAFETONIGHT"

We'll use the pad I have given you. She takes her copy of the pad. It's the first message, so use the text on Page 1. We take as many letters as we need to match the message length, which is 22.

It means our text, and our "keyword" is

M	E	E	T	M	E	A	T	T	H	E	C	A	F	E	T	O	N	I	G	H	T
B	D	U	F	G	H	W	E	I	U	F	G	W	E	I	U	F	B	W	E	J	N

So Alice writes this table down. Next, convert the letters into their number equivalent. We get:

12	4	4	19	12	4	0	19	19	7	4	2	0	5	4	19	14	13	8	6	7	19
1	3	20	5	6	7	22	4	8	20	5	6	22	4	8	20	5	1	22	4	9	13

since M corresponds to 12, E corresponds to 4, and so on.

Now do the modular arithmetic. We add together the two rows (mod 26). So for example, we start with the first column and do 12 + 1 = 13 (mod 26). Going through the whole table, we get:

13	7	24	24	18	11	22	23	1	1	9	8	22	9	12	13	19	14	4	10	16	6

Now convert these into the corresponding letters:

N	H	Y	Y	S	L	W	X	B	B	J	I	W	J	M	N	T	O	E	K	Q	G

and so this is the encrypted message “NHYYSLWXBBJIWJMNTOEKQG”

Remember, she now destroys this first page. This means the only copy of the first page is now with Bob, there were only two to start with, and Alice just destroyed hers.

Decrypting using the one-time pad

Bob gets the message and needs to work it out. He takes his pad and writes the coded message on top of the same “keyword” which he reads from his pad (remember, Alice and Bob’s pads are identical).

N	H	Y	Y	S	L	W	X	B	B	J	I	W	J	M	N	T	O	E	K	Q	G
B	D	U	F	G	H	W	E	I	U	F	G	W	E	I	U	F	B	W	E	J	N

Again, he converts to numbers:

13	7	24	24	18	11	22	23	1	1	9	8	22	9	12	13	19	14	4	10	16	6
1	3	20	5	6	7	22	4	8	20	5	6	22	4	8	20	5	1	22	4	9	13

But instead of adding like Alice did, he does the opposite, which is subtracting. So he subtracts the rows (mod 26). For example, he starts with 13 – 1 = 12 (mod 26), then 7 – 3 = 4 (mod 26) and so on. He gets

12	4	4	19	12	4	0	19	19	7	4	2	0	5	4	19	14	13	8	6	7	19

When checking this, don’t forget that things like 1 - 8, which is -7, are equivalent to 19 (mod 26), since -7 = (-1) × 26 +19 – you need to remember this and practice with it if it’s taking you more time.

Finally, convert into letters and, as we hoped, we get

M	E	E	T	M	E	A	T	T	H	E	C	A	F	E	T	O	N	I	G	H	T

Bob now destroys his page. There are no copies now existing of the “keyword” (Alice and Bob have destroyed the only two copies) and so no-one in the world knows the keyword, and no-one can possibly know it in the future since it was randomly created and now destroyed completely.

Weaknesses of the one-time pad

In practice, the one-time pad has several weaknesses.

- Only Alice and Bob have the pad. But what happens if someone steals it? How do we make sure that no-one interrupts them while they create the pad? If someone does get a copy of the pad, then it's easy for them to decrypt.

- Suppose one message got lost in transmission. Suddenly Alice and Bob are working on different sheets. Alice sent a message and destroyed a page. But Bob never got it, so he didn't throw away his page. So they are on different pages now.

- Each "keyword" **must** only be used once. If even one page is ever used again, patterns may be created and hacking may be possible, at least to an expert.

- Randomness. How do you create random letters? Have a look at the pad I gave you. I created this by just randomly pressing buttons on my keyboard for a while. But is this *truly* random? Look at the first line, the string "WEIUF" appears twice. Page 2 is even worse. That wasn't intended, it's just how my fingers worked. Also the keyboard letters aren't equally distributed, a human tendency is to stray away from Q or P or M, for example, as they don't have letters all around them, Q is next to the "tab" button, M is next to the comma button. Try it for yourself, sit at a computer and try and type away. Do you really feel that you are generating a totally random sequence? The question of how to generate a truly random sequence is tricky. Computers don't work randomly, when you generate "random numbers" on a computer they are actually subject to a complex formula based on a "seed" number, which only appear random. Generating absolutely truly random sequences is very, very difficult.

- Fundamentally, how do you deal with the practicalities of creating a pad that only Alice and Bob have a copy of, and where the pages can be securely destroyed forever?

Historical use of the one-time pad

The one-time pad was used fairly extensively before the Second World War. The pad was often of the size as illustrated on the picture earlier, much smaller than your palm. The pages would often be made out of a combustible paper, so that when you had used them, they were easy to totally destroy (burn them).

One of the most famous examples of the one-time pad was the Venona project, which you can research on for the tutorial exercises. The key of the breaking of this, was that due to the amount of work in producing keywords, pages were not completely destroyed and were later re-used. That basic mistake renders the one-time pad almost as easy to crack as such ciphers as a substitution or Vigenère cipher (the fundamentals are the same).

Summary

The one-time pad uses modular arithmetic – theoretically it may be perfect, but it has flaws. It's another step forward on our tour through historical cryptography but we still have a long way to go!