Simple Cryptosystems and Attacks

Ahto Buldas

September 10, 2018

Cryptosystem

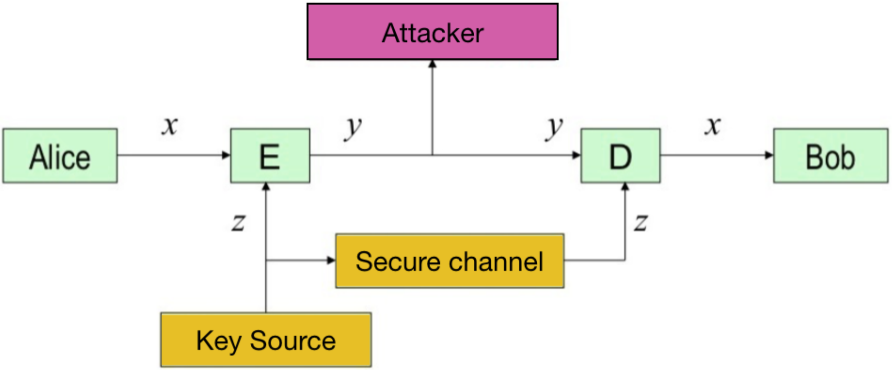
$\mathbf{X}$ – set of all possible plaintexts
$\mathbf{Y}$ – set of all possible ciphertexts
$\mathbf{Z}$ – set of all possible keys

Encryption and Decryption: For every $z \in \mathbf{Z}$, there are functions

$$E_z \colon \mathbf{X} \to \mathbf{Y} \qquad \text{and} \qquad D_z \colon \mathbf{Y} \to \mathbf{X} \ ,$$

such that $D_z(E_z(x)) = x$ for every $x \in \mathbf{X}$

Encrypted Communication



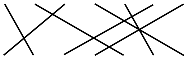
Kerckhoffs assumption: If given z, attacker can compute E_z and D_z

Secrecy: Attacker must not be able to deduce x from y.

Permutation Cipher

Letters of the message are permuted

`M E S S A G E` ⟵ Plaintext



⟵ Key

`S M G E E A S` ⟵ Ciphertext

$\mathbf{X}$ – all possible n-letter texts
$\mathbf{Z}$ – all possible ways of permuting the letters of the message

$$|\mathbf{Z}| = n! = 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n$$

Substitution Cipher

Every letter is substituted with another letter, by using a table:

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

For example a plaintext `MESSAGE` is encrypted to `ORAAQWR`:

M	E	S	S	A	G	E
O	R	A	A	Q	W	R

$\mathbf{X}$ – all possible texts
$\mathbf{Z}$ – all possible permutations of the 26-letter alphabet

$$|\mathbf{Z}| = 26! = 2 \cdot 3 \cdot \ldots \cdot 25 \cdot 26 \approx 2^{88}$$

Shift Cipher

Circular shift of the alphabet

For example, *Julius Caesar* (100–44 a.d.) used shift by three:

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

$\mathbf{X}$ – all possible texts
$\mathbf{Z}$ – all possible shifts of the 26-letter alphabet

$|\mathbf{Z}| = 26$

Computers and Cryptography

Convert letters to numbers:

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

Shift cipher $y = E_z(x)$, where $x, y, z \in \{0, 1, 2, \ldots, 25\}$:

$$y = E_z(x) = x + z \bmod 26 = \begin{cases} x + z & \text{if } x + z < 26 \\ x + z - 26 & \text{if } x + z \geq 26 \end{cases}$$

General shift cipher $y = E_z(x)$, where $x, y, z \in \{0, 1, 2, \ldots, n-1\}$:

$$y = E_z(x) = x + z \bmod n = \begin{cases} x + z & \text{if } x + z < n \\ x + z - n & \text{if } x + z \geq n \end{cases}$$

One-Time Pad

Use shift cipher

Encrypt every letter x with a different, independently chosen random key z

$\mathbf{X}$ – all possible n-letter messages: $x_1 x_2 \ldots x_n$
$\mathbf{Z}$ – all possible n-letter keys: $z_1 z_2 \ldots z_n$
$\mathbf{Y}$ – all possible n-letter ciphertexts: $y_1 y_2 \ldots y_n$

$$y_i = x_i + z_i \mod 26$$

Unbreakable: ciphertext contains no information about the plaintext, except its size

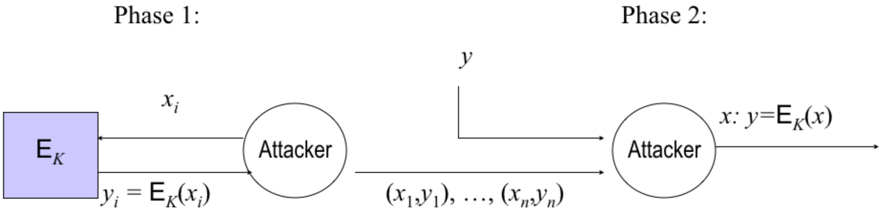
Main Attacking Strategies

- *Trial decryption*, using all possible keys. Need to recognize the right key!
- *Derivation* using plaintext-ciphertext pairs
- *Language statistics* may be transferred from plaintext to ciphertext

Passive Attacks

- *Known ciphertext*: attacker knows a ciphertext Y
- *Known plaintext*: attacker knows plaintext-ciphertext pairs $(X_1, Y_1), \ldots, (X_n, Y_n)$

Active attacks: Chosen Plaintext



Active attacks: Chosen Ciphertext