Lecture 4

Symmetric encryption and perfect secrecy

Nicola Laurenti October 9, 2020

Lecture 4— Contents

General model of an encryption system

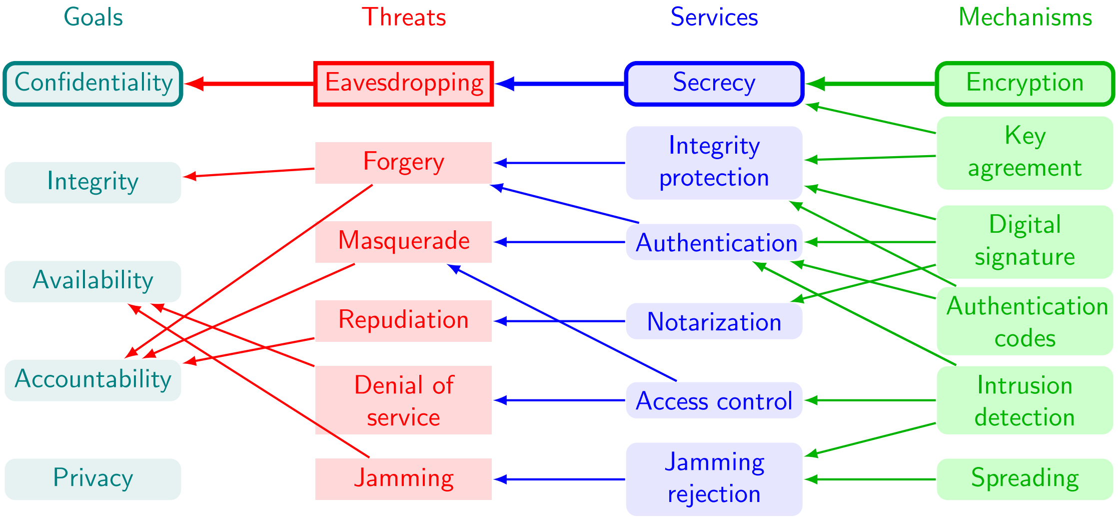
The guessing attack

- Success probability
- Sequential guessing

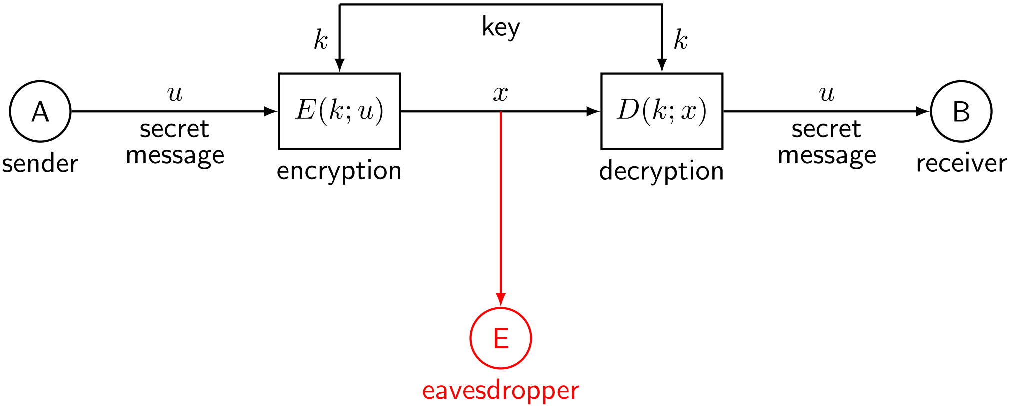
Perfect secrecy

- Definition
- One-time pad

Security goals, threats, services and mechanisms



General model of an encryption system



Glossary and notation

secret message (plaintext) $u \in \mathcal{M}$ message space

transmitted message (ciphertext) $x \in \mathcal{X}$ cipher space

encryption key $k \in \mathcal{K}$ key space

encryption map $E : \mathcal{K} \times \mathcal{M} \mapsto \mathcal{X}$

$$E_k : \mathcal{M} \mapsto \mathcal{X} \quad E_k(u) \doteq E(k, u)$$

decryption map $D : \mathcal{K} \times \mathcal{X} \mapsto \mathcal{M}$

$$D_k : \mathcal{X} \mapsto \mathcal{M} \quad D_k(x) \doteq D(k, x)$$

Key and plaintext are random with probability mass distribution

key pmd $p_k : \mathcal{K} \mapsto [0, 1]$ typically uniform: $k \sim \mathcal{U}(\mathcal{K})$

plaintext pmd $p_u : \mathcal{M} \mapsto [0, 1]$ not necessarily uniform

The encryption system is completely specified as $\mathcal{S} = (\mathcal{M}, \mathcal{X}, \mathcal{K}, E, D, p_u, p_k)$

General assumptions

- (perfect reliability)The receiver must be able to recover the secret message perfectly

$$D_k = E_k^{-1} \quad \forall k \in \mathcal{K}$$

- (Kerchoff's assumption) The eavesdropper knows the system $\mathcal{S}$ (in particular the maps $E(\cdot,\cdot)$ and $D(\cdot,\cdot)$)

Where does secrecy come from?

Secrecy is only based on the fact that the eavesdropper does not know the actual realization of k and hence the particular $E_k(\cdot)$, $D_k(\cdot)$ used

A simple example

LA RIVISTA CHE VANTA INNUMEREVOLI TENTATIVI D'IMITAZIONE!

LA SETTIMANA ENIGMISTICA

10 Luglio 2014 — N. 4294 — Anno 83 — Euro 1,50 (in Italia)

ESCE IL GIOVEDÌ

39118. L'ANEDDOTO CIFRATO

1 2 3 4 5 6 7 7 3 4 8 9
— 7 6 — 1 7 9 5 machine 8
10 — 11 4 — 12 3 1 10 4 9
— 8 10 — 3 5 7 3 4 5 10
12 City, 1 9 4 9 — 1 5 3 5
6 — 13 6 12 11 14 6 13 3
5 6 — 7 6 — 2 9 4 6 5 10
4 6 — 12 15 6 — 4 6 16 7
10 anni 6 13 3 4 9 — 1 12
10 17 9 7 3 5 6 — 10 4 —
7 11 9 16 15 10 inaccessibili 3
10 — 12 7 10 6 4 5 10 : —
10 7 — 7 9 13 9 valore 5 9
5 3 7 6 — 6 13 3 — 8 10
— 2 10 16 7 10 3 10 3 — 8
10 — 8 9 7 7 3 13 10 .

Sostituite una lettera ad ogni numero.

Example (Substitution cipher)

$$\mathcal{M} = \bigcup_{\ell \in \mathcal{L}} \mathcal{A}_u^\ell = \mathcal{A}_u^* \quad , \qquad \mathcal{X} = \mathcal{A}_x^*$$

$$E_k \; : \; [x_1, \ldots, x_\ell] = [e_k(u_1), \ldots, e_k(u_\ell)]$$

$$\text{with } e_k \; : \; \mathcal{A}_u \mapsto \mathcal{A}_x \text{ injective}$$

Provided $|\mathcal{A}_u| \leq |\mathcal{A}_x|$, the class $\{e_k\}$ of all injective functions $\mathcal{A}_u \mapsto \mathcal{A}_x$ has cardinality

$$K = \prod_{i=1}^{|\mathcal{A}_u|} (|\mathcal{A}_x| - i + 1) = \frac{|\mathcal{A}_x|!}{(|\mathcal{A}_x| - |\mathcal{A}_u|)!}$$

We can take $\mathcal{K} = \{1, \ldots, K\}$. If $|\mathcal{A}_u| = |\mathcal{A}_x| = M$, then $K = M!$

The guessing attack

In this attack, E wants to learn the value of u, and attempts a guess $\hat{u} \in \mathcal{M}$

Ignorant guess

By ignoring the reading of x, the optimal guess for E is

$$\hat{u} = \arg\max_{a \in \mathcal{M}} p_u(a) \quad = P(u = a)$$

and the corresponding success probability is

$$\mathrm{P}\left[\hat{u} = u\right] = p_u(\hat{u}) = \max_{a \in \mathcal{M}} p_u(a)$$

Informed guess

By making use of her knowledge of x, the optimal guess for E is a function of x

$$\hat{u} = g(x)$$

x = Agosto, caldo

with

$$g : \mathcal{X} \mapsto \mathcal{M} \quad g(b) = \arg\max_{a \in \mathcal{M}} p_{u|x}(a|b)$$

and the corresponding success probability is

$$\begin{aligned} \mathrm{P}\left[\hat{u} = u\right] = \mathrm{P}\left[g(x) = u\right] &= \sum_{b \in \mathcal{X}} \mathrm{P}\left[g(x) = u | x = b\right] p_x(b) \\ &= \sum_{b \in \mathcal{X}} p_{u|x}(g(b)|b) p_x(b) = \sum_{b \in \mathcal{X}} p_x(b) \max_{a \in \mathcal{M}} p_{u|x}(a|b) \end{aligned}$$

In general, it is not lower than the ignorant guess, as

$$\sum_{b \in \mathcal{X}} p_x(b) \max_{a \in \mathcal{M}} p_{u|x}(a|b) \geq \max_{a \in \mathcal{M}} \sum_{b \in \mathcal{X}} p_x(b) p_{u|x}(a|b) = \max_{a \in \mathcal{M}} p_u(a)$$

Sequential guessing

If E has a means to check the correctness of her guess she can repeat guesses $\hat{u}_i, i = 1, 2, \ldots$ until she hits the correct plaintext. The optimal choice for the i-th ignorant guess is recursively defined as

$$\hat{u}_i = \begin{cases} \arg\max\limits_{a \in \mathcal{M}} p_u(a) & , \quad i = 1 \\ \arg\max\limits_{a \in \mathcal{M} \setminus \{\hat{u}_1, \ldots, \hat{u}_{i-1}\}} p_u(a) & , \quad i > 1 \end{cases}$$

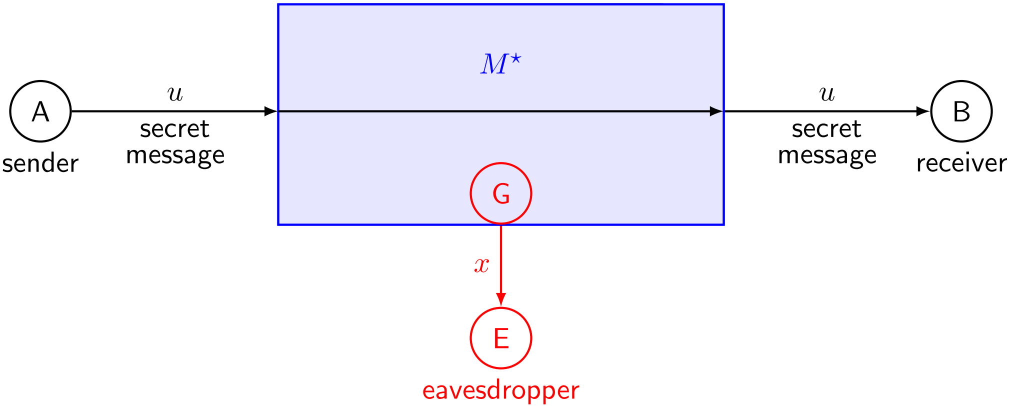
while for informed guesses

$$\hat{u}_i = g_i(x) \quad , \quad g_i(b) = \begin{cases} \arg\max\limits_{a \in \mathcal{M}} p_{u|x}(a|b) & , \quad i = 1 \\ \arg\max\limits_{a \in \mathcal{M} \setminus \{\hat{u}_1, \ldots, \hat{u}_{i-1}\}} p_{u|x}(a|b) & , \quad i > 1 \end{cases}$$

The attack performance is evaluated in terms of

- probability of success in or before N guesses: $\mathrm{P}\left[\cup_{i=1}^{N} \hat{u}_i = u\right] = \sum_{i=1}^{N} \mathrm{P}\left[\hat{u}_i = u\right]$
- statistics of the number of attempts before success

Ideal world model

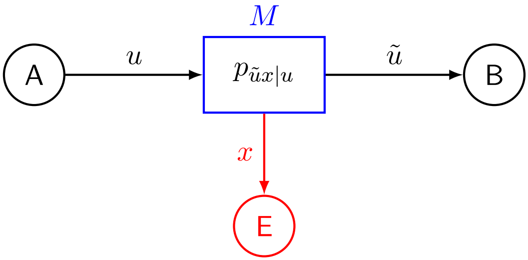


In the ideal counterpart of encryption, the secret message u is directly delivered, unmodified to B, and the message observed by E is generated independently from u

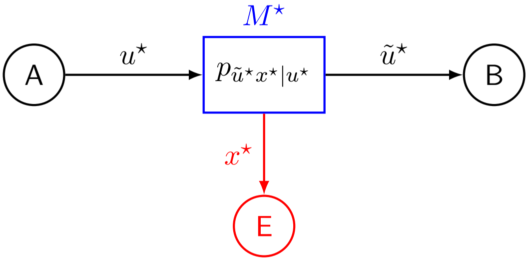
Perfect Secrecy

The best we can hope for, is an encryption system M that is statistically identical to its ideal counterpart $M^\star$

real



ideal



$$
\begin{aligned}
p_{\tilde{u}x|u}(b,c|a) &= p_{\tilde{u}^\star x^\star|u^\star}(b,c|a) \\
\text{(independence)} &= p_{\tilde{u}^\star|u^\star}(b|a)\,p_{x^\star}(c) \\
\text{(correctness)} &= \delta(a,b)\,p_{x^\star}(c)
\end{aligned}
$$

Perfect Secrecy

Definition

An encryption system is perfect if it provides 0-unconditional security based on indistinguishability, i.e. the plaintext is statistically independent of the ciphertext

$$p_{x|u}(b|a) = p_x(b) \quad \forall a \in \mathcal{M}, b \in \mathcal{X}$$

or equivalently

$$p_{ux}(a,b) = p_u(a)p_x(b) \quad \forall a \in \mathcal{M}, b \in \mathcal{X}$$
$$p_{u|x}(a|b) = p_u(a) \quad \forall a \in \mathcal{M}, b \in \mathcal{X}$$

In a system with perfect secrecy, since $p_{u|x} = p_u$ the optimal informed guessing strategy coincides with the optimal ignorant guessing

One-time pad

Let $(\mathbb{G}, \circ)$ be a finite group, [e.g., $(\mathbb{Z}_N, + \bmod N)$]. A one-time pad (OTP) over $(\mathbb{G}, \circ)$ is the encryption system described by

equal spaces $\mathcal{M} = \mathcal{X} = \mathcal{K} = \mathbb{G}$

uniform key $k \sim \mathcal{U}(\mathbb{G}) \quad \Leftrightarrow \quad p_k(a) = \frac{1}{|\mathbb{G}|} \, \forall a \in \mathbb{G}$

encrypt by add $E(a, b) = b \circ a$

decrypt by subtract $D(a, c) = c \circ a^{-1}$

Example

Let $\mathbb{G} = \mathbb{B}^N$, with $\mathbb{B} = \{0, 1\}$, $N = 5$, and $\circ =$ bitwise XOR. Then, e.g.,

$$u = 01101, k = 10110 \quad \Rightarrow \quad x = u \circ k = 11011$$

B can recover the message with $k^{-1} = k = 10110$

$$u = x \circ k^{-1} = 01101$$

Secrecy of one-time pad

Theorem

The one-time pad offers perfect reliability and perfect secrecy for any message distribution

Proof.

Perfect reliability is guaranteed by the existence and uniqueness of $k^{-1} \in \mathbb{G}$.
As regards perfect secrecy, we prove that $p_{u,x}(b,c) = p_u(b)p_x(c), \forall b \in \mathcal{M}, c \in \mathcal{X}$. In fact,

$$
\begin{aligned}
p_{u,x}(b,c) &= \mathrm{P}\left[u = b, x = c\right] = \mathrm{P}\left[u = b, k = b^{-1} \circ c\right] \\
&= p_u(b)p_k(b^{-1} \circ c) = p_u(b)/|\mathcal{K}| \\
p_x(c) &= \sum_{b \in \mathcal{M}} p_{u,x}(b,c) = \sum_{b \in \mathcal{M}} p_u(b)/|\mathcal{K}| = 1/|\mathcal{K}|
\end{aligned}
$$

Observe that this result holds for any $p_u(\cdot)$. □

Summary

In this lecture we have:

- introduced a general model for symmetric encryption
- discussed guessing attacks
- defined perfect secrecy
- presented a mechanism that achieves it

Assignment

- class notes
- textbook, §3.1–§3.3

End of lecture

this comic reproduced from xkcd URL: xkcd.com/257