

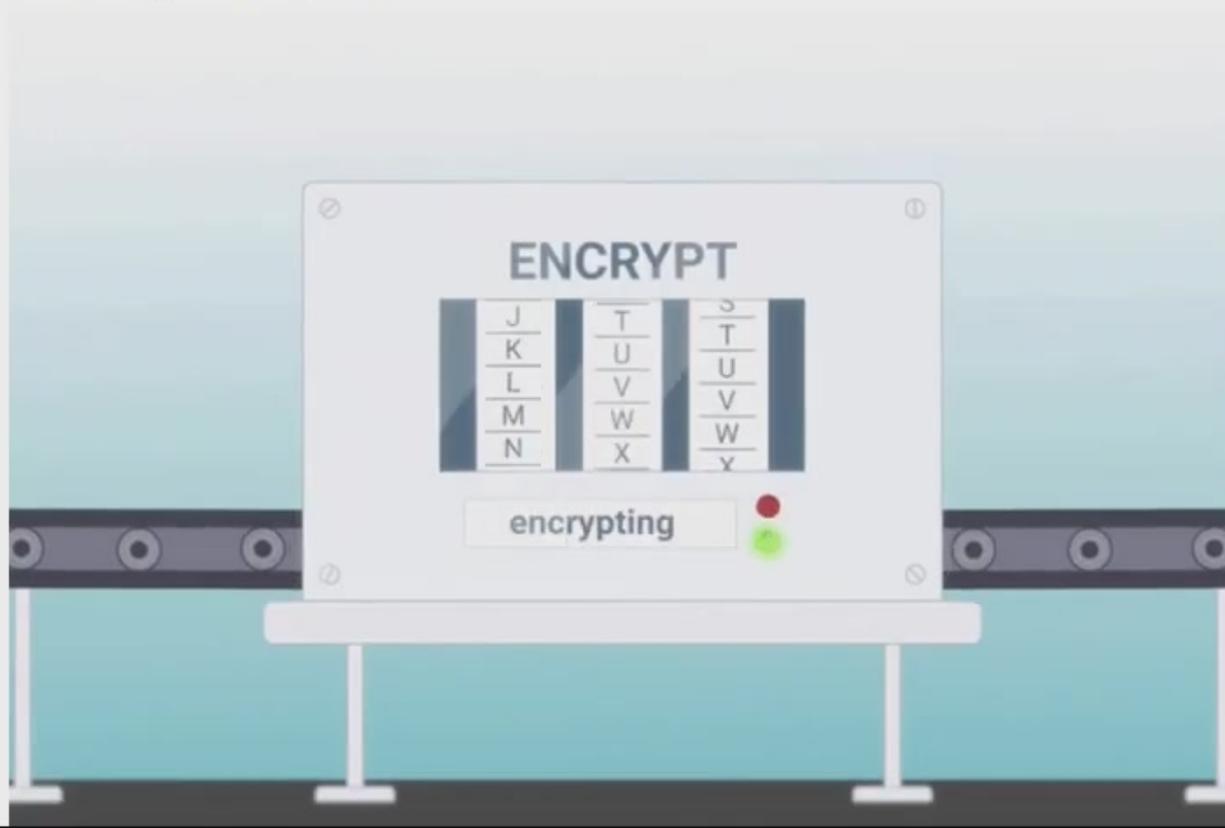
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



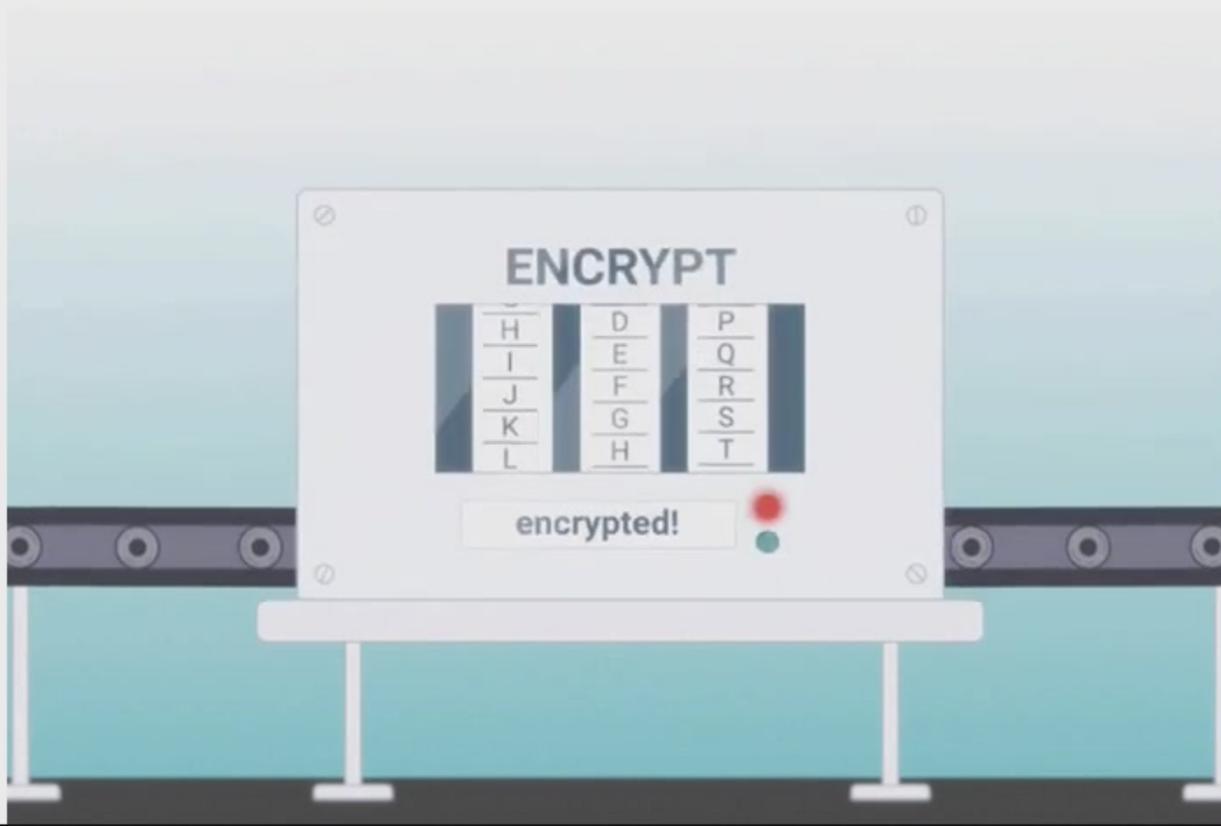
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



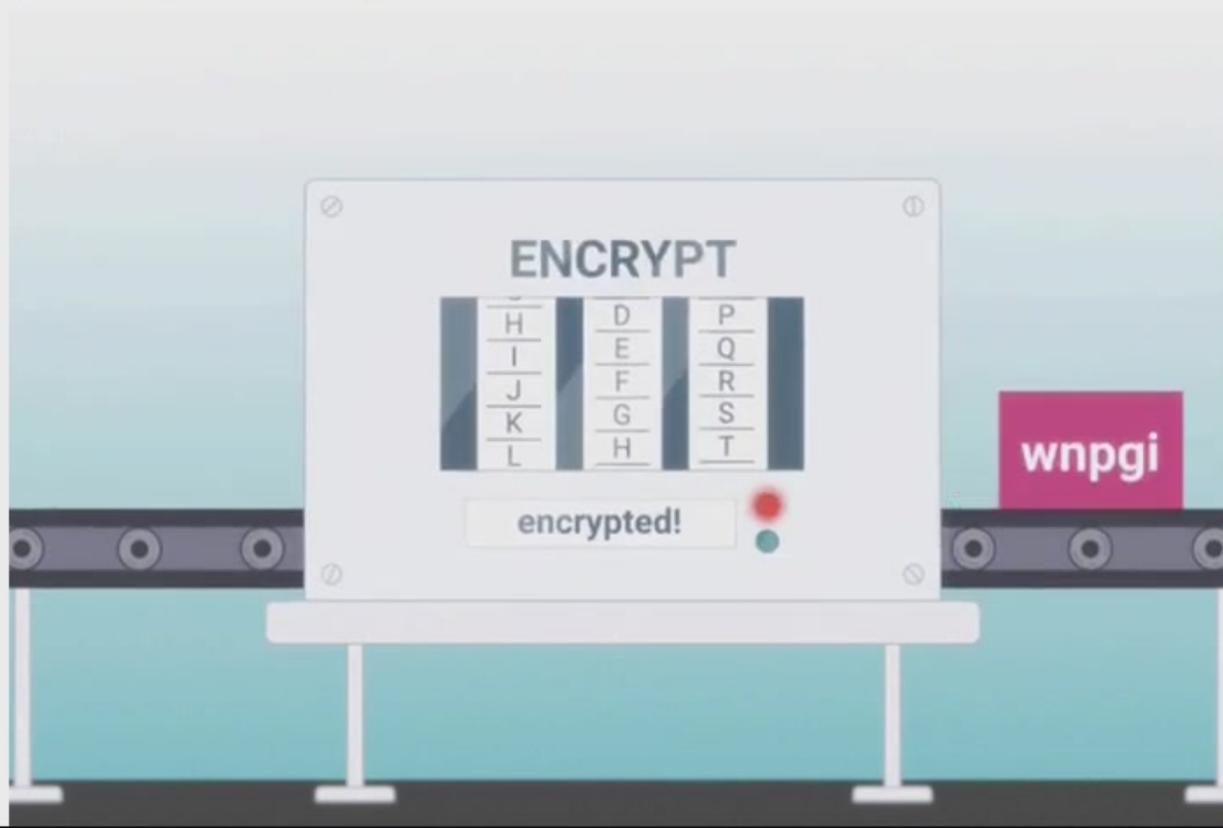
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



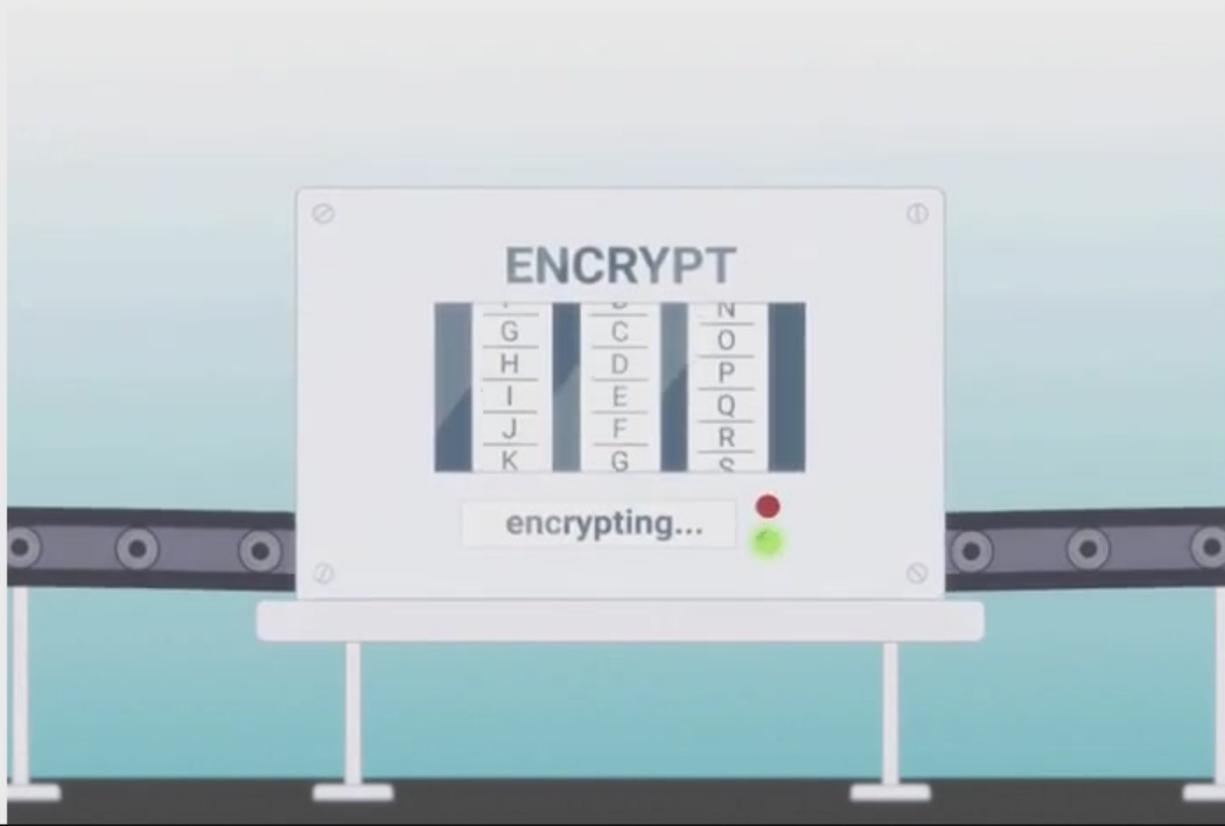
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



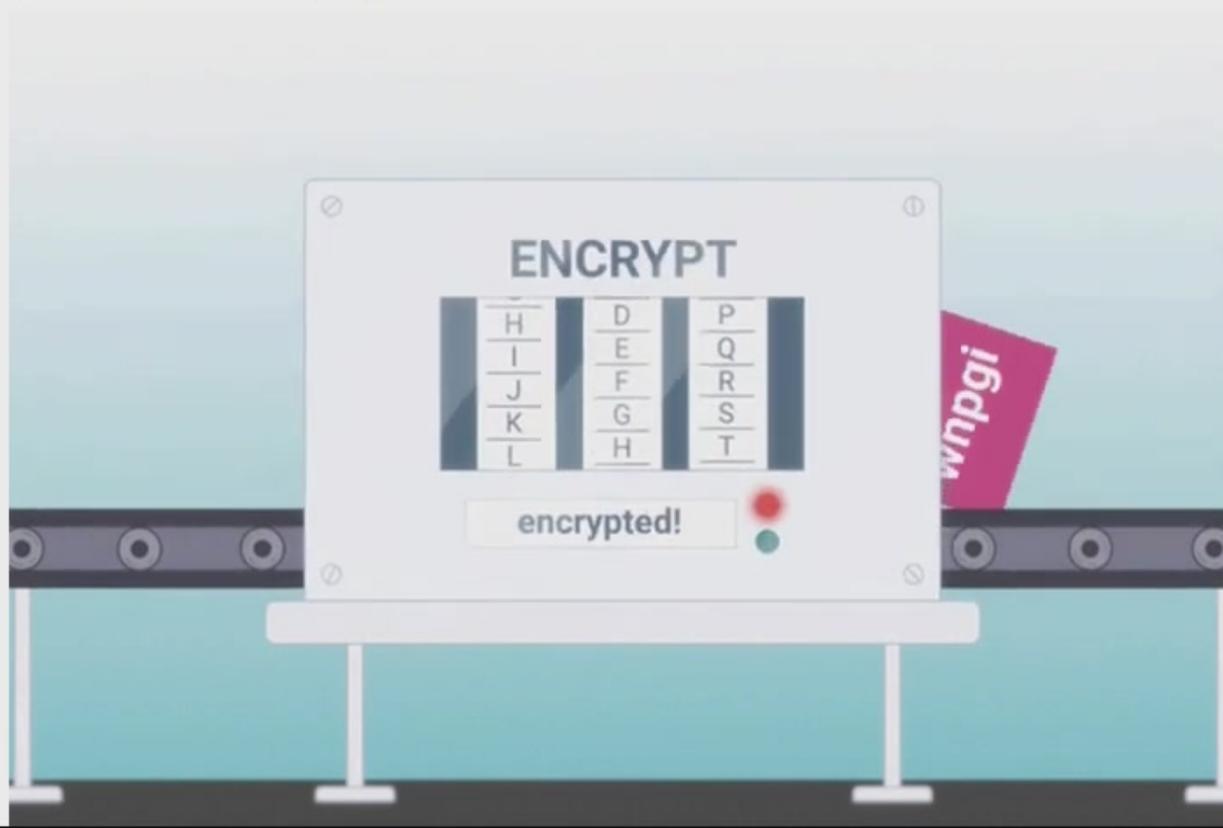
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



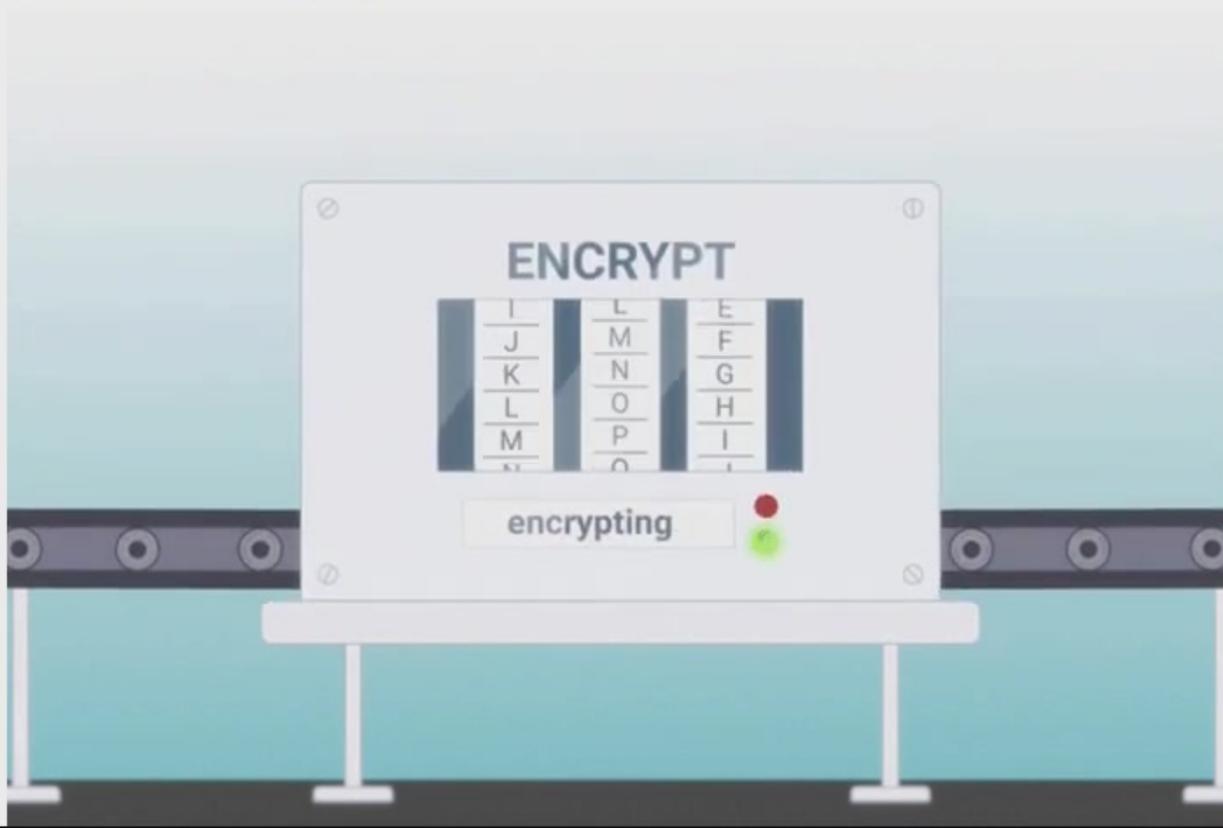
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



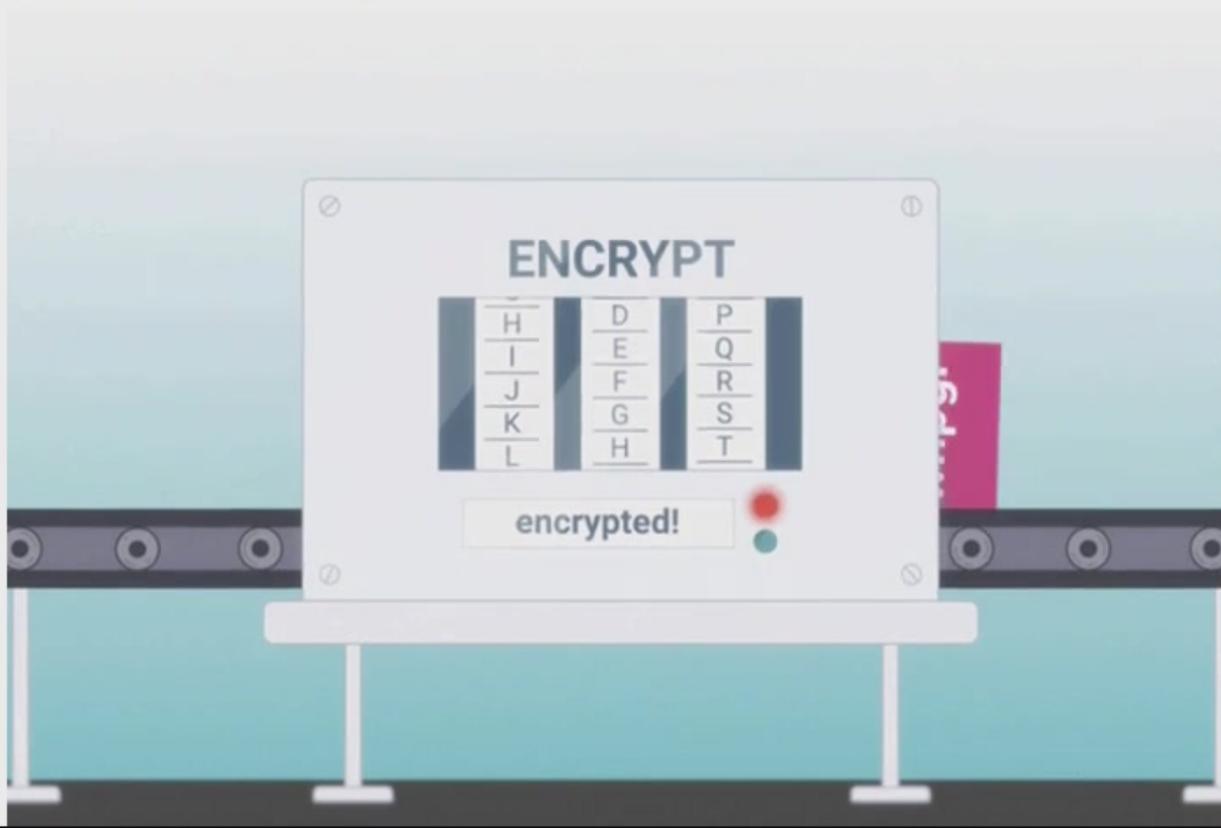
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



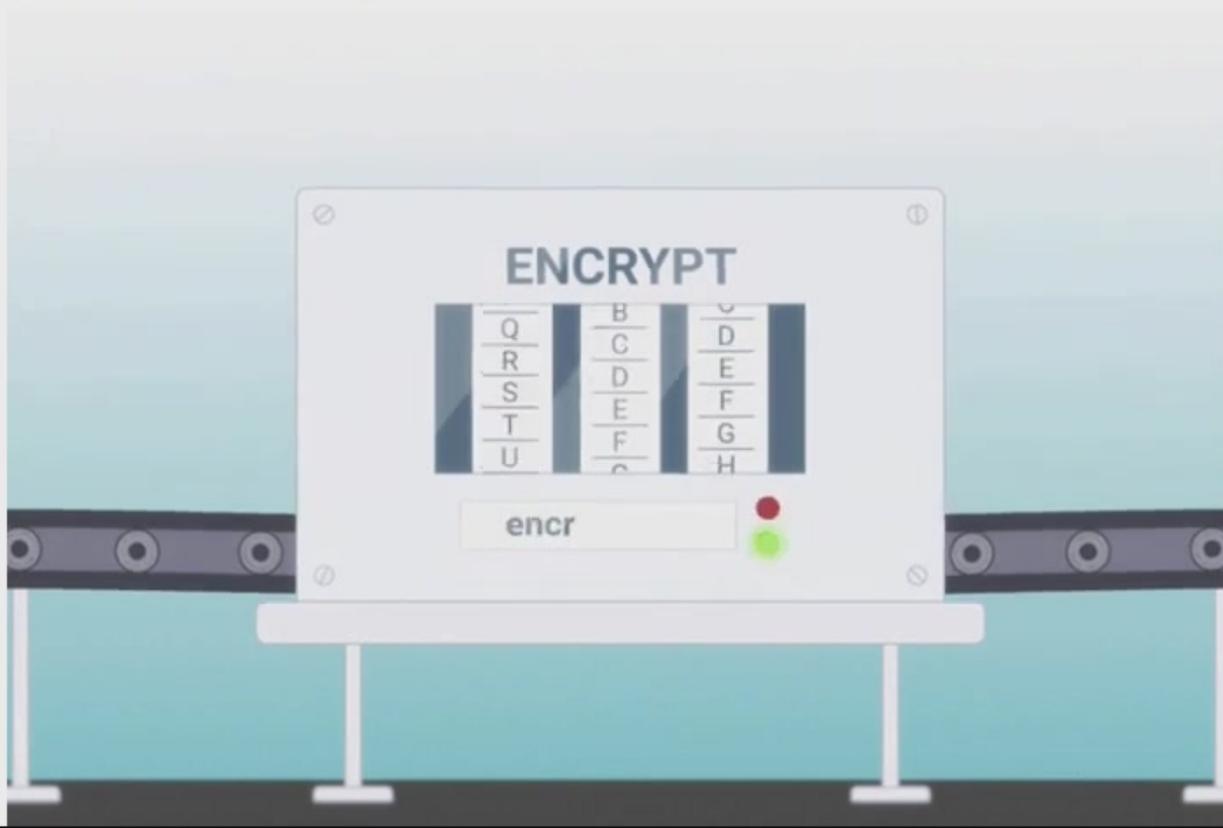
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



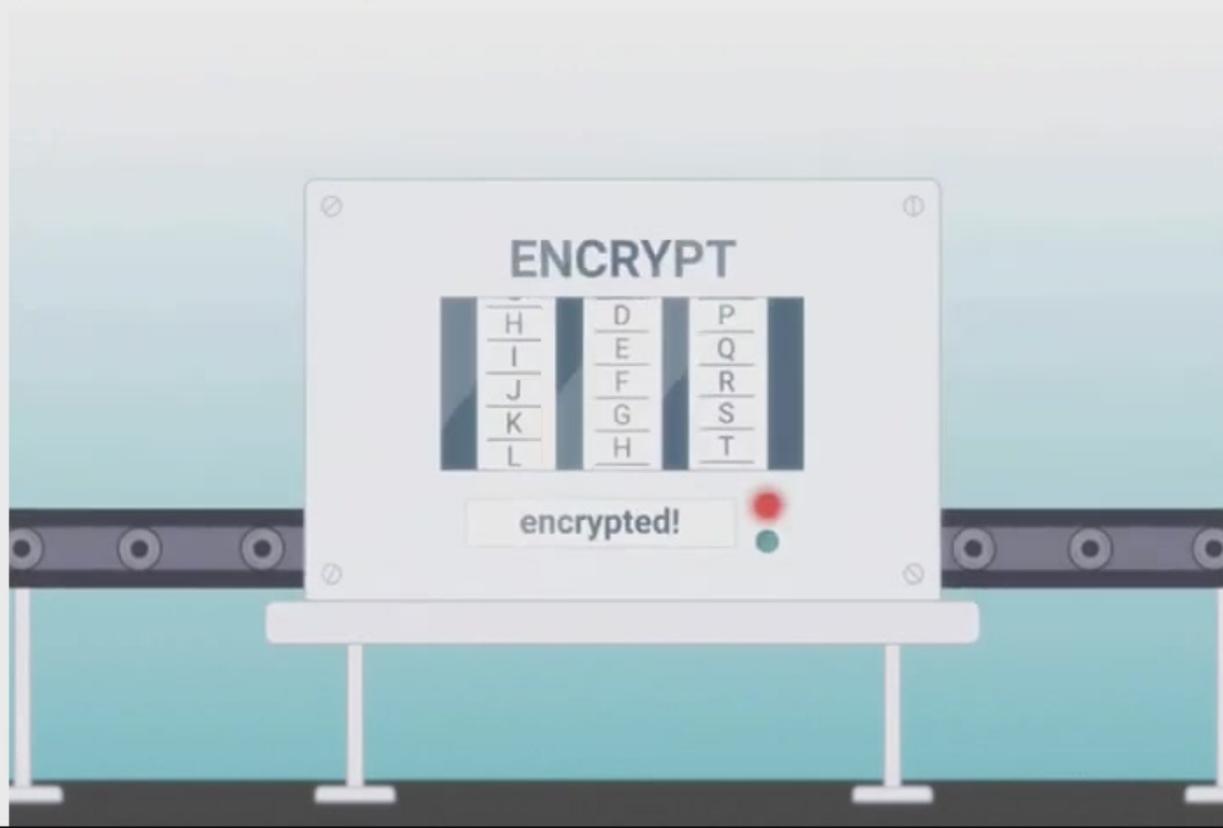
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



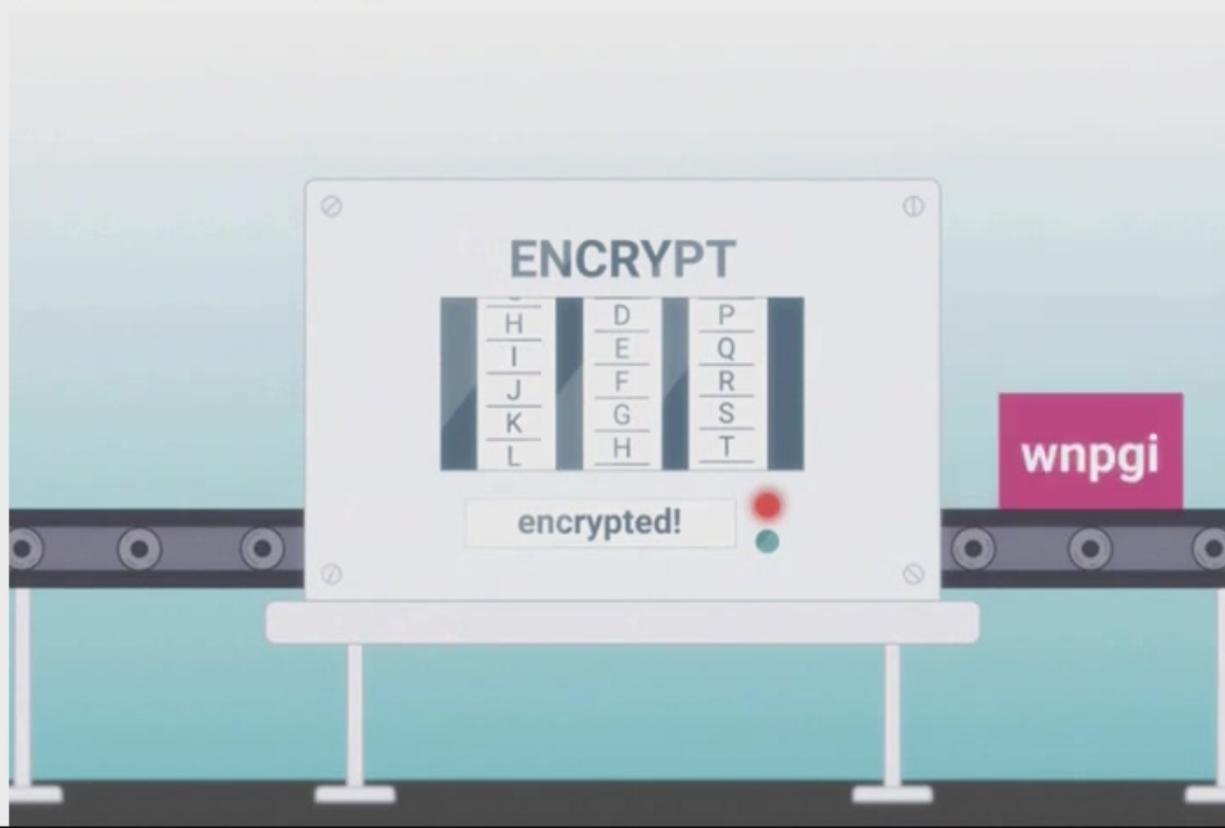
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

κρυπτογραφία μελετά τρόπους εξασφάλισης της εμπιστευτικότητας

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

κρυπτογραφία μελετά τρόπους εξασφάλισης της εμπιστευτικότητας

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

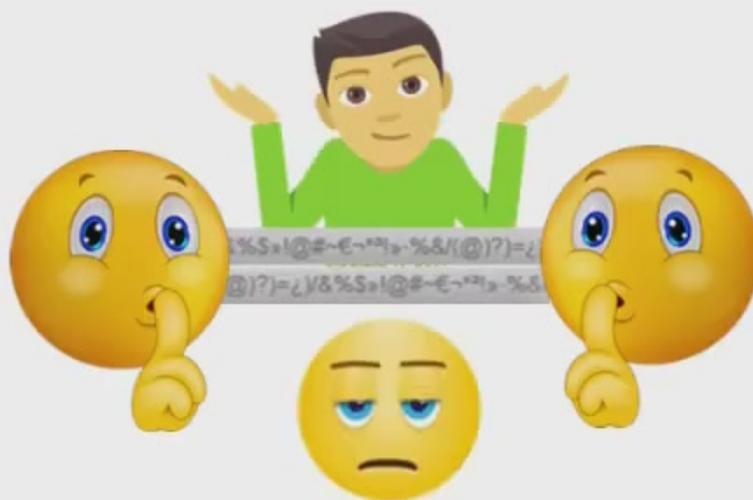
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας**
στην **ΕΠΙ**



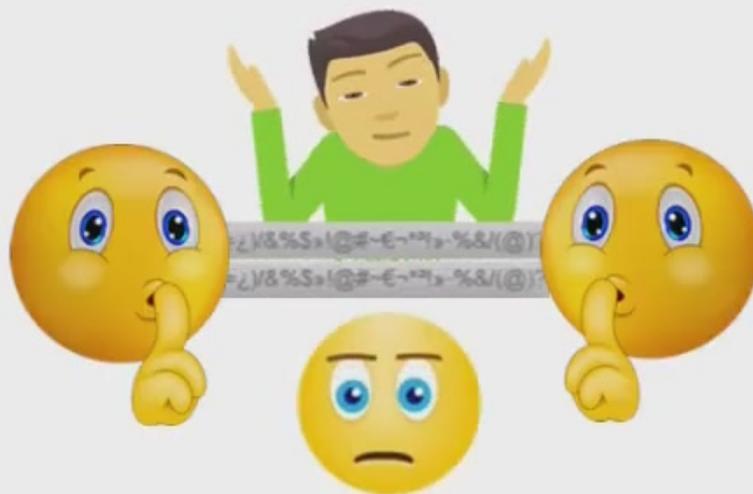
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

κρυπτογραφία μελετά τρόπους **εξασφάλισης** της εμπιστευτικότητας στην **επικοινωνία** δυο πλευρών.



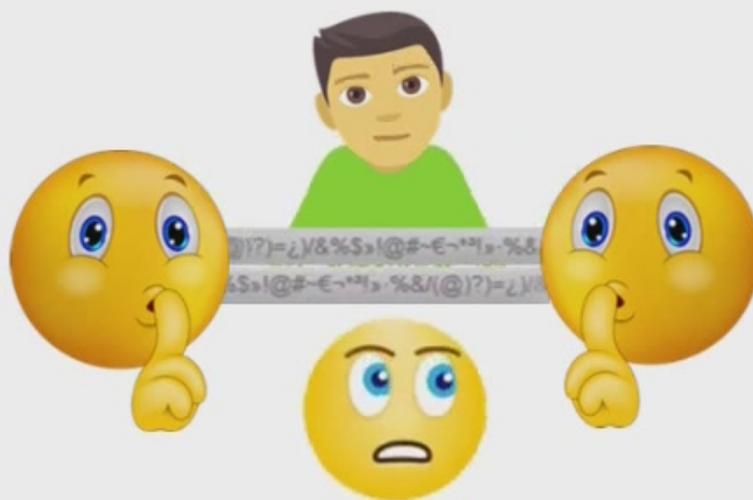
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας** στην **επικοινωνία** δυο πλευρών.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

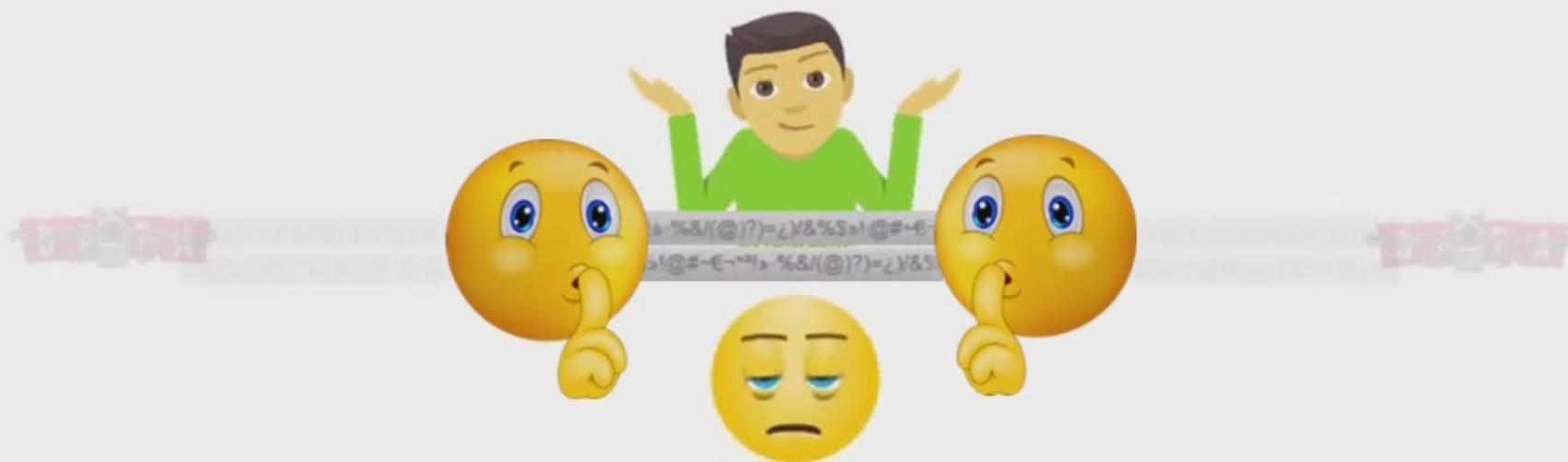
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας** στην **επικοινωνία** δυο πλευρών.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

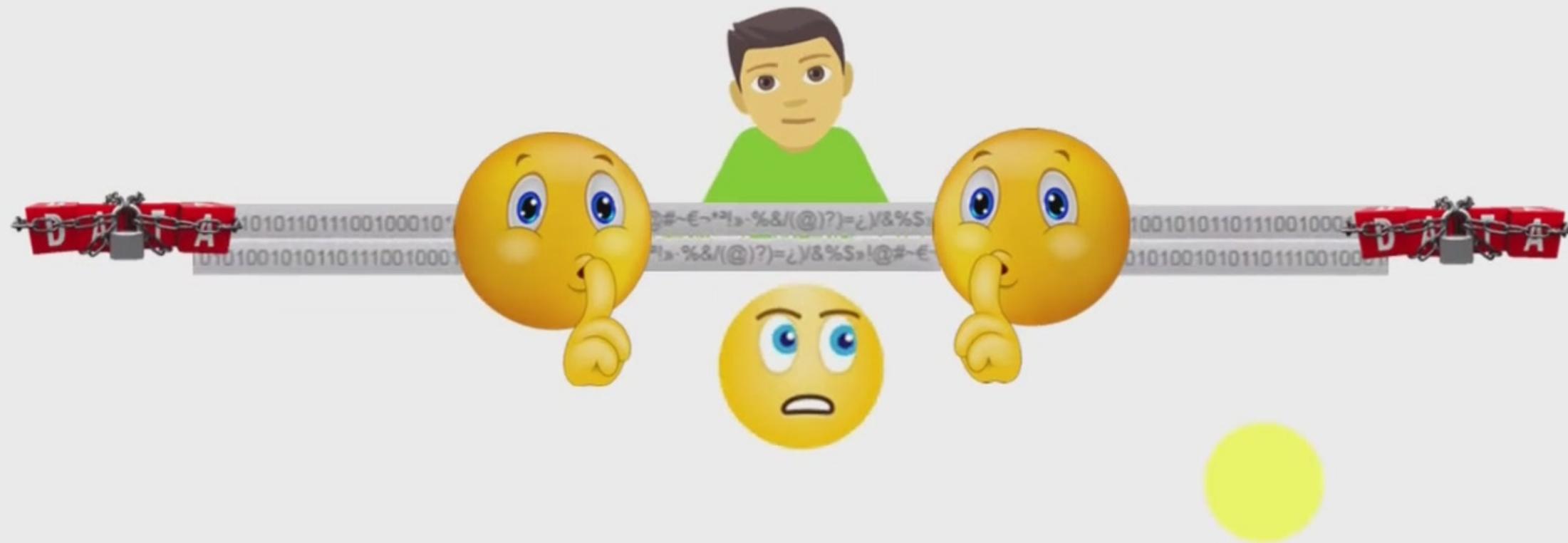
κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας** στην **επικοινωνία** δυο πλευρών.



Περίληψη Λογισμικού

Κρυπτογραφία (Cryptography)

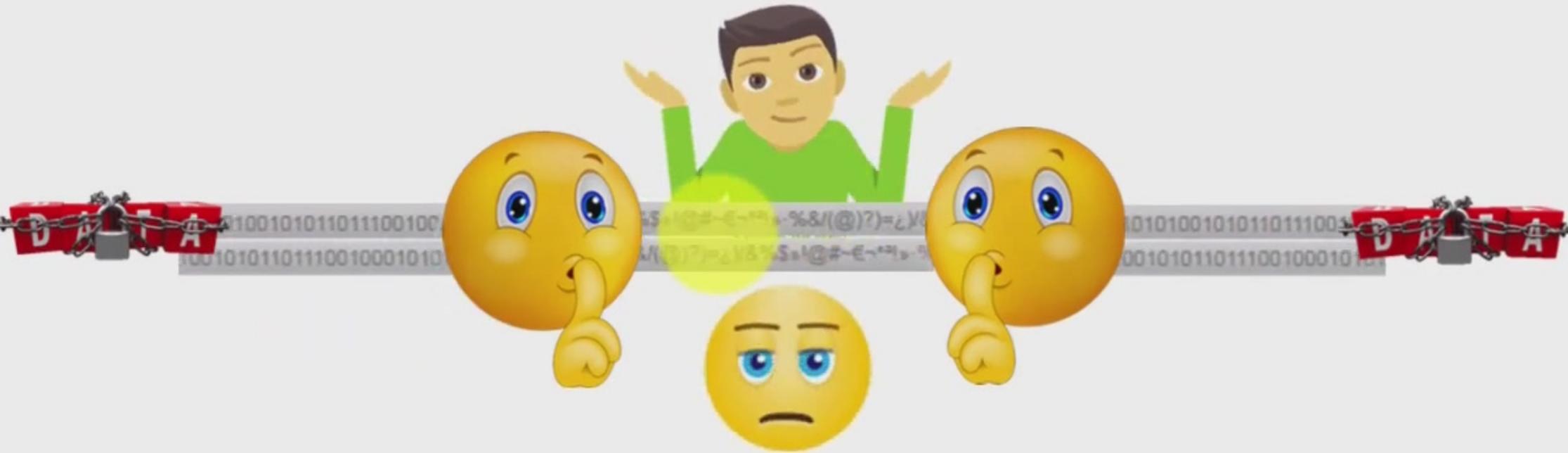
Κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας**
επικοινωνία δυο πλευρών.



Λειτουργία Λογισμικού

Κρυπτογραφία (Cryptography)

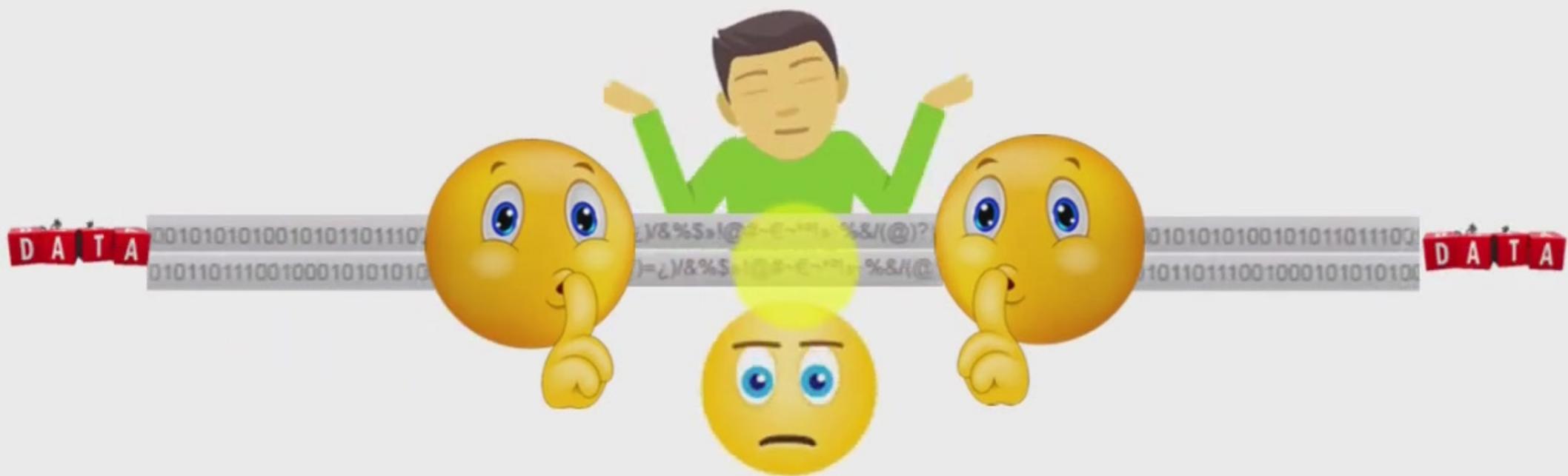
Κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας** της **επικοινωνίας** δυο πλευρών.



Μεθοδολογία Λογισμικού

Κρυπτογραφία (Cryptography)

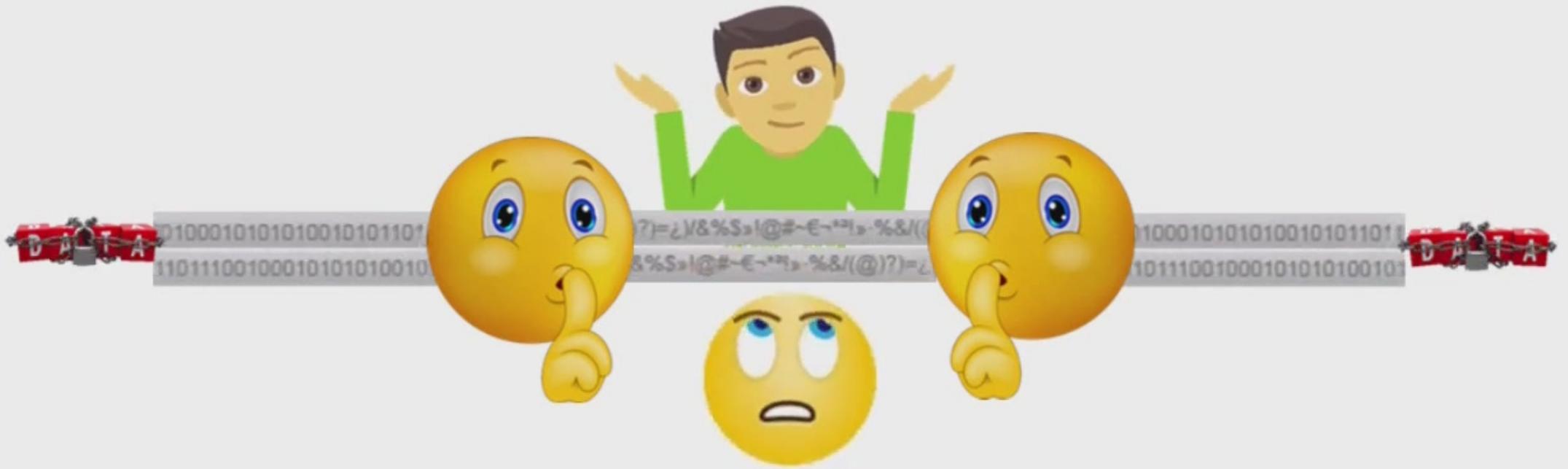
Κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας** της **επικοινωνίας** δυο πλευρών.



Λειτουργία Λογισμικού

Κρυπτογραφία (Cryptography)

Κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας** της **επικοινωνίας** δυο πλευρών.



ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

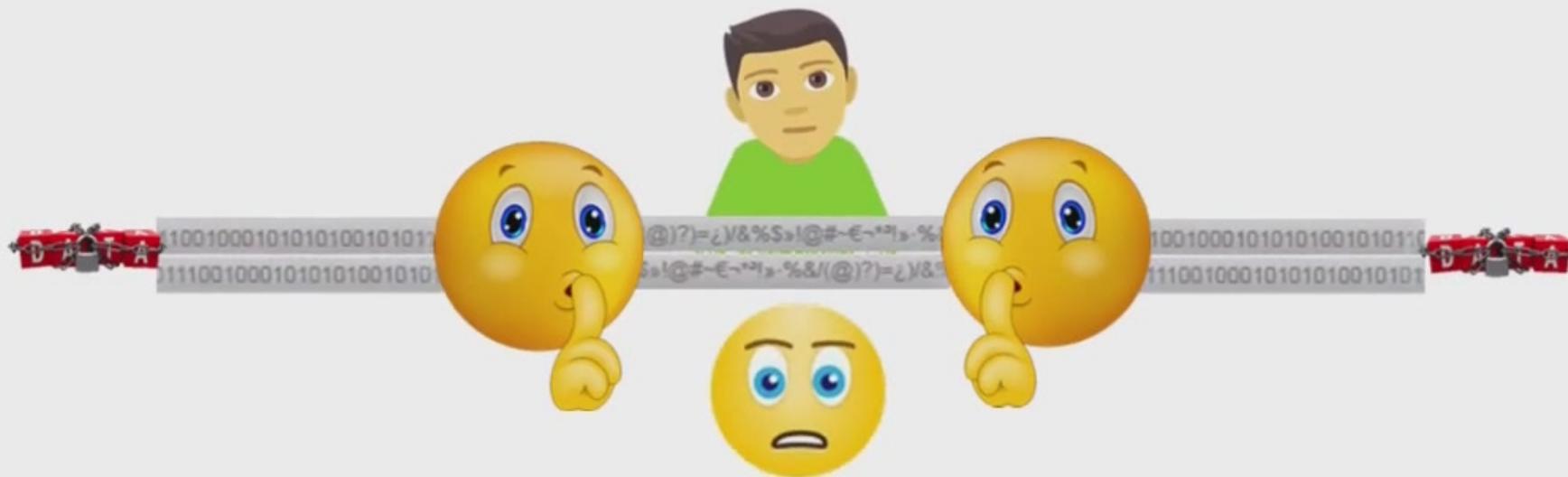
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

3 Ασφάλεια Λογισμικού

3.4 Κρυπτογραφία (Cryptography)

κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας** στην **επικοινωνία** δυο πλευρών.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

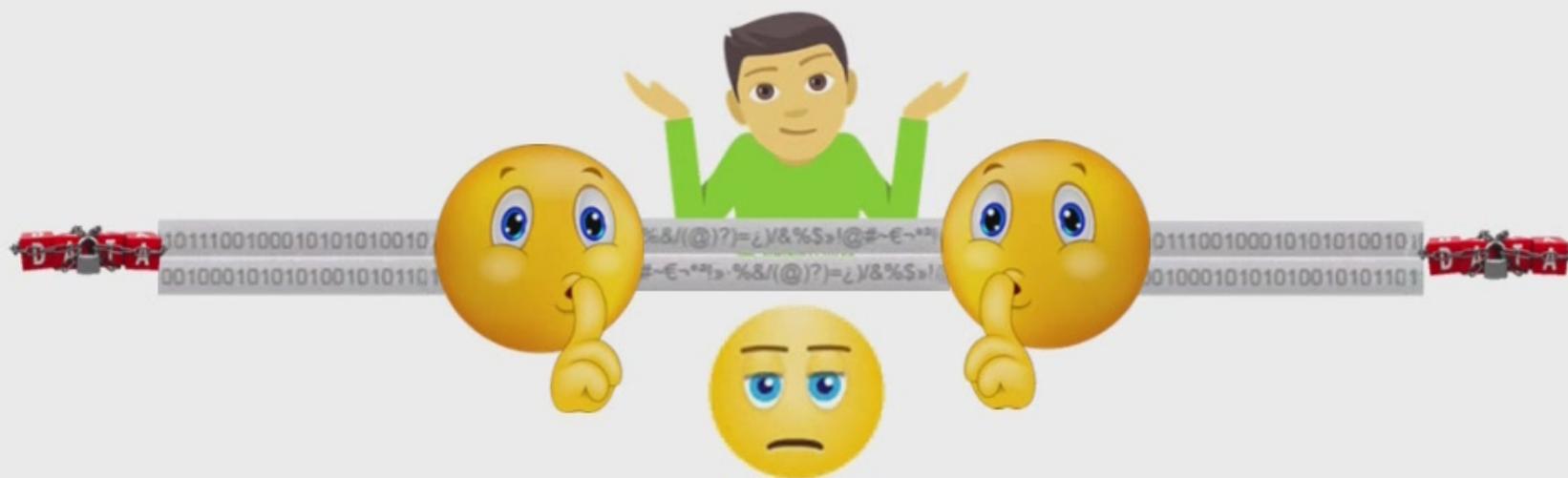
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας** στην **επικοινωνία** δυο πλευρών.



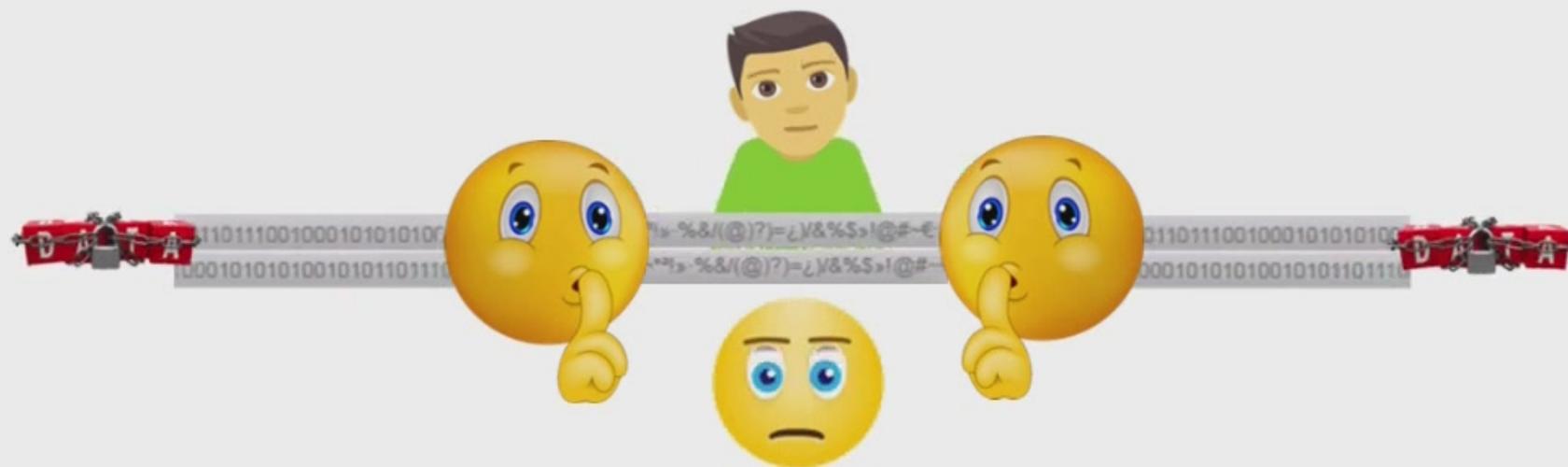
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

κρυπτογραφία μελετά τρόπους **εξασφάλισης** της **εμπιστευτικότητας** στην **επικοινωνία** δυο πλευρών.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

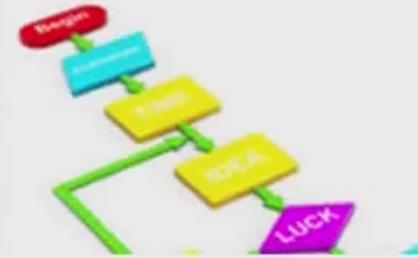
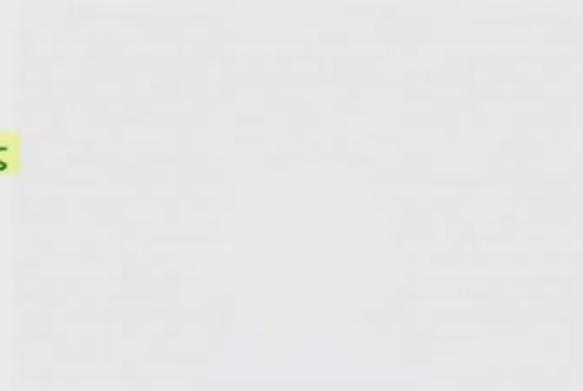
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Για να υλοποιηθούν οι αλγόριθμοι κρυπτογράφησης



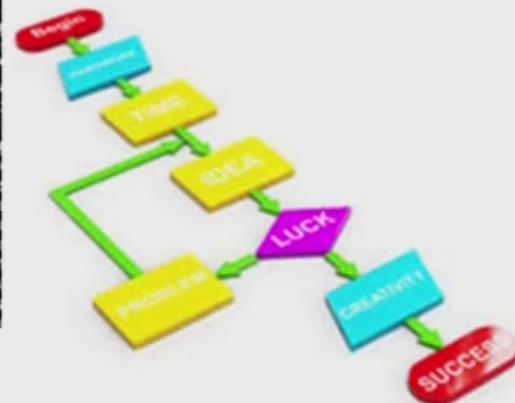
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

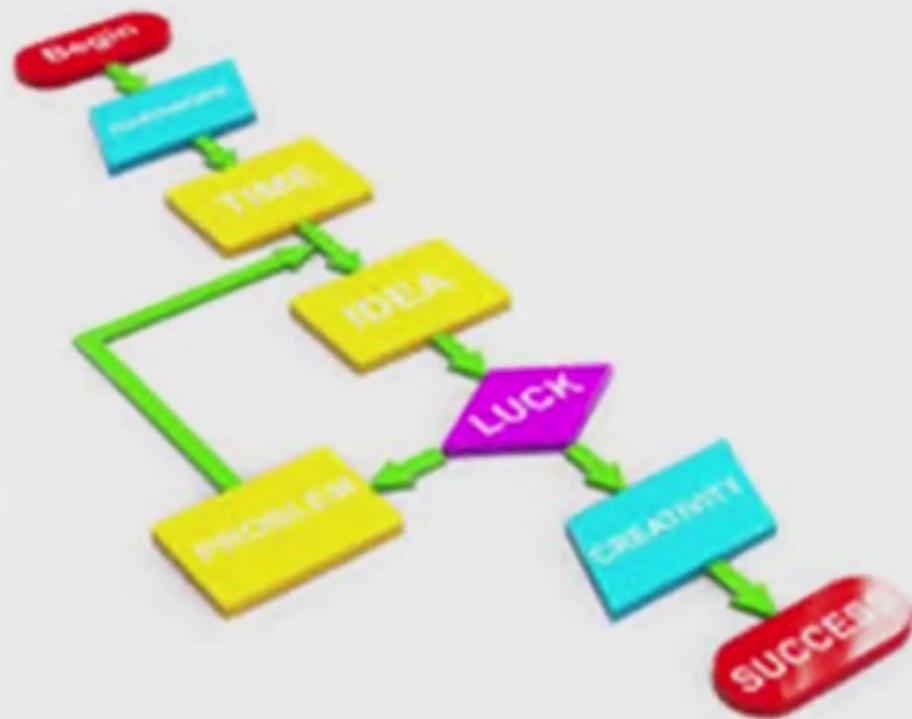
5.3.4 Κρυπτογραφία (Cryptography)

Για να υλοποιηθούν οι αλγόριθμοι κρυπτογράφησης



Πληροφοριακών Συστημάτων

γράφησης



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

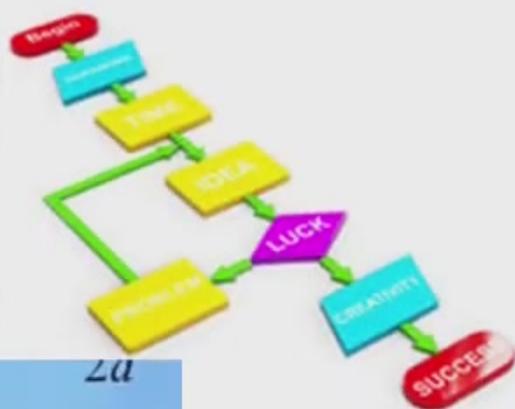
Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Για να υλοποιηθούν οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται μαθηματικά όπως:

```
(r.to(t)):n=t?this.pause().cycle():this.slide(t>n?"next":t<n?"prev":this.cycle(!0)),clearInterval(this.interval),this.interval=null;this.slide("prev")}lide("next"));prev:function(){if(thive"),i=n||r[t()],s=this.interval,o="next?"left":"right";e.slide("slide",{rehis.pause(),i=i.length?i:this.$element.$indicators.length&&(this.$indicators.find(".active").addClass("active"))});ar t=e(a.$indicators.children()[a.$element.trigger(f);if(e.support.transition){class([t,o].join(" "));e.support.transition()});a.sliding=!1,seon(){a.$element.trigger("e"),this.sliding=!1,seon();r.removeClass("active");var n=e.fn.carousel.prototype.cycle(n){return this;eof n=="string"?n:sel.defaults.type,to(n);o?i[o]():s.i.cycle());},e.fn.carousel({return e.fn.carousel.prototype.constructor=t,e.fn.carousel}, [data-slide-to",function var n=e(this),i=e(n.o),{o:n.attr("data-slide-to"),extend(i,i.data()),f:Default}})(window,e){"use strict";vent=e(this,option);return n;ults_n).this.on
```



$e^{j\pi} + 1 = 0$

$X_k = \frac{1}{N} \sum_{n=0}^{N-1} x_n e^{i2\pi kn}$

$\Delta = \frac{\sqrt{4a^2 + (CI \times \dots)}}{\delta_{ij}}$

$y = \sum_{i=0}^{10} x_i$

$\frac{P(E_e|H_h) P(H_h)}{P(E_e)}$

Κεφάλαιο 5ο

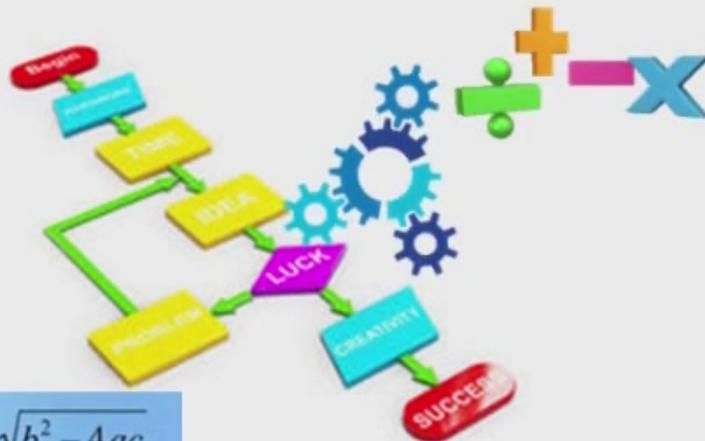
Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Για να υλοποιηθούν οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται μαθηματικά όπως: πρώτοι αριθμοί,

```
r.to(t)):n=t?this.pause().cycle():this.slide(t>n?"next":this.end&paused=!0),this.$element.find(".next,.prev").cycle(!0),clearInterval(this.interval),this.interval=null,de("prev"))||de("next"))},prev:function(){if(this.sliding,i=n||r[t](),s=this.interval,o="next?"+"left":"right","slide",{rehis.pause(),i=i.length?i:this.$element.find("this.$indicators.length&&(this.$indicators.find(".active":active"))}ar t=(a.$indicators.children()[a.getActiveIn:s.$element.trigger(f);if(a.defaultPrevented())return;.join(" ")$element.on("transition.end",function(){a.sliding=!1,sevented(a.$element.trigger("sliding=!1,tevented(a.$element.trigger("Class("active"),i.advar n=e.fn.carousel.prototype.cycle(n){return this.ring"?n:s.send({});},ts,typeof n=="objeto(n):o?i[o]():s.interval(a.cycle()));},e.fn.carousel.carousel.Constructor.prototype.cycle);e.fn.carousel.noConflict(),[data-slide-to",function(){var n=(this),r=i(e(n).r("data-sli+$"),""),i=i.data(),n.data(),dDefault({}))}(window).on("load",function(){e("use strict";v:is,options.pa,e.fn.carousel.defaults,options.paren
```



$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Euler's Identity

$$e^{ix} + 1 = 0$$
$$X_k = \frac{1}{N} \sum_{n=0}^{N-1} x_n e^{i2\pi k \frac{n}{N}} = \frac{\sqrt{PA^2 + (CI \times N_c)^{\Delta}}}{\delta_{ij}}$$
$$\int_a^b f(x) dx$$
$$P(H_h|E_e) = \frac{P(E_e|H_h)P(H_h)}{P(E_e)}$$
$$y = \sum_{i=0}^{10} x_i$$

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Για να υλοποιηθούν οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται μαθηματικά όπως: πρώτοι αριθμοί, ημίπρωτοι,

```
r.to(t));n=t?this.pause().cycle():this.slide(t>n?"next":this.support.transition.end&paused=!0),this.$element.find(".cycle(!0),clearInterval(this.interval),this.interval=null,turn this.slide("prev")}lide("next")),prev:function(){if("ve",i=n||r[t](),s=this.interval,o="next"?left:"right"),f=e.slide("slide",{rehis.pause(),i=i.length?i:this.$e this.$indicators.length&&(this.$indicators.find(".active" t.addClass("active"))))ar t=e(a.$indicators.children())s.$element.trigger(f);if(!e.support.transition())return; veClass([t,o].join(" ")," "));e(e.support.transition " ")),a.sliding=!1,se on(){a.$element.trig tive"),this.sliding=!1,se on(){a.$element.trig var n=e.fn.carousel.prototype.transition(n){return thi typeof n="string"rousel.defaults,ty to(n):o?i[o]():s.ile cycle()}},e.fn.ca n(){return e.fn.carousel.prototype.constructor=t,e.fn.care ], [data-slide-to",fun var n=e(this),r,i=e(n.a l(s),{omn.attr("data Default{}))}(wind e)}{"use strict";v parent=(this.on defaults,n).this,
```


$$X_k = \frac{1}{N} \sum_{n=0}^{N-1} x_n e^{i2\pi kn}$$
$$P = \frac{\sqrt{PA^2 + (C \delta_{ij})}}{\delta_{ij}}$$
$$y = \sum_{h=0}^{10} H_h P(H_h)$$

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Για να υλοποιηθούν οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται μαθηματικά όπως: πρώτοι αριθμοί, ημίπρωτοι, παραγοντοποίηση κ.λπ.

```
r.to(t));n=t?this.pause().cycle():this.slide(t>n?"next":this.$element.find(".next", ".prev").length&&e.support.transition?this.cycle(!0),clearInterval(this.interval),this.interval=null},prev:function(){if(this.sliding)return;return this.slide("prev",i=n||r[t](),s=this.interval,o="next?"left":"right",i=i.length?i:this.$element.find(".item")[u](),f=e.slide(this.$indicators.length&&(this.$indicators.find(".active").indicators.children()[a.getActiveIndex()]);t&&t.addClass("prev"),s.$element.trigger(f);if(e.support.transition){s.$element.trigger(e.support.transition("prev"));i.removeClass(["active","prev"]);a.sliding=!1,setTimeout(function(){a.$element.trigger("slid");r.removeClass("prev"),t.addClass("active"),this.cycle();},e.support.transition("prev")?this.interval:0)},return;r.removeClass("prev"),t.addClass("active"),this.cycle();},var n=e.fn.carousel.defaults,o=typeof n=="string"?n:n||{};e.fn.carousel.prototype=e.extend({},e.fn.carousel.defaults,{constructor:t,e.fn.carousel.prototype},[e.extend({},i.data("carousel"),{o:n,at:Default})]);(window.jQuery)"use strict";(function(){var n={};n.parent=(this);
```


$$X_k = \frac{1}{N} \sum_{n=0}^{N-1} x_n e^{i2\pi k \frac{n}{N}}$$
$$B_s = \frac{\sqrt{PA^2 + (C \delta_i)^2}}{\delta_i}$$
$$y = \sum_{h=0}^{10} \dots$$
$$\frac{P(H_h)}{P(H_h)}$$

Κεφάλαιο 5ο

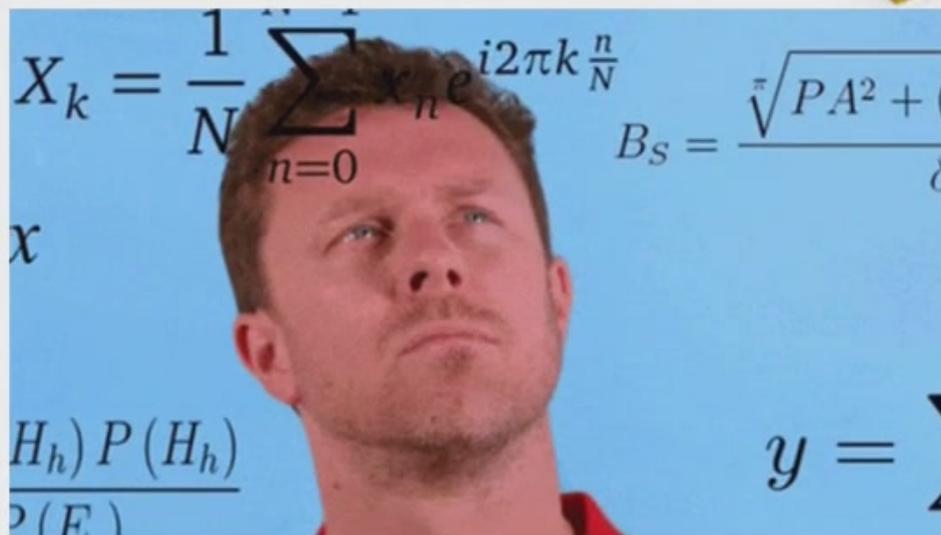
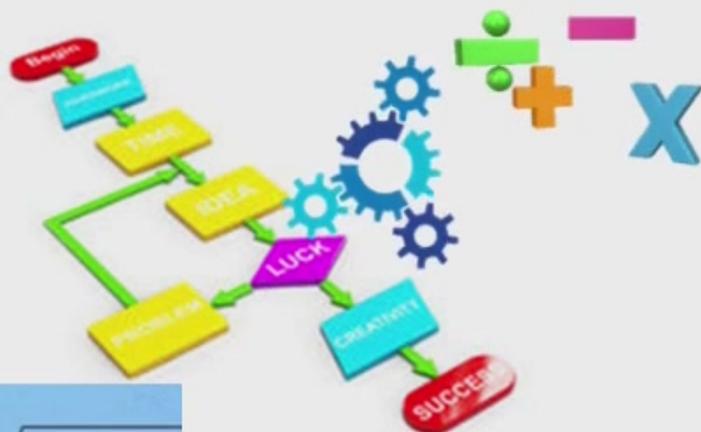
Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Για να υλοποιηθούν οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται μαθηματικά όπως:
πρώτοι αριθμοί,
ημίπρωτοι,
παραγοντοποίηση κ.λπ.

```
r.to(t)):n=t?this.pause().cycle():this.slide(t>n?"next":  
end&pause=!0),this.$element.find(".next,.prev").length  
cycle(!0)),clearInterval(this.interval),this.interval=null  
("next")),prev:function(){if(this.sliding)return  
ve",i=n||r[t](),s=this.interval,o="next?"+"left":"right",  
{rehis.pause(),i=i.length?i:this.$element.find(".item")  
this.$indicators.length&&(this.$indicators.find(".active  
))}ar t=e(a.$indicators.children()[a.getActiveIndex()])  
s.$element.trigger(f);if(!defaultPrevented())return;  
")$element.one(e.suppressEvent,function(){i.r  
"},a.sliding=!1,setTimeout(function(){a.$element.trig  
!1,tevented()}return  
var n=e.fn.carousel.prototype.cycle(n){return thi  
s.send({},e.fn.carousel.prototype.cycle(n));  
to(n);o?i[o]():s.interval=this.cycle()}},e.fn.carousel  
usel.carousel.Constructor.prototype.cycle=function  
el,[data-slide-to],function n(e=this),r,i=e(n.a  
-sli)+$/,""),s=e.owl.carousel({items:1,n.data(),o:i,caro  
Default({})})(window).owl.carousel({useStrict:true;v  
s.on,e.fn.carousel.prototype.cycle(n);parent&&(this
```



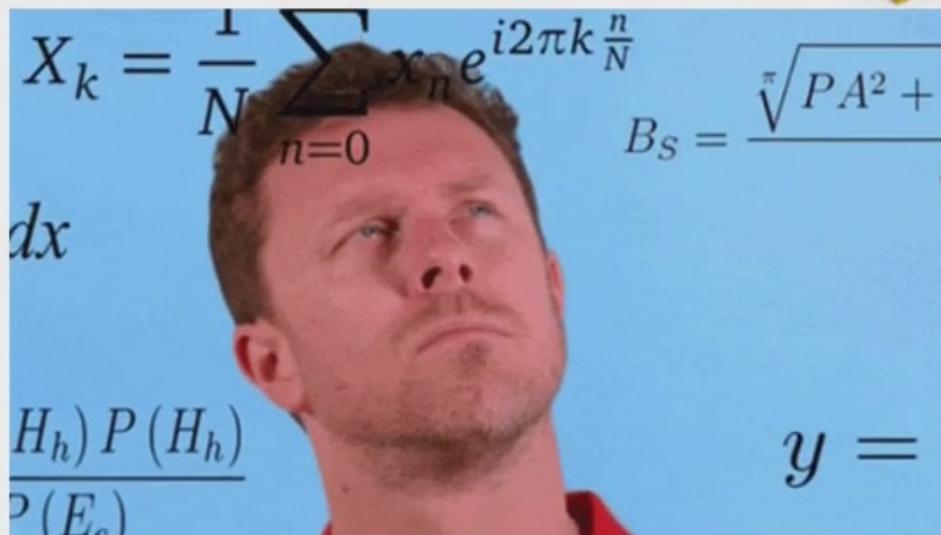
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Για να υλοποιηθούν οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται μαθηματικά όπως:
πρώτοι αριθμοί,
ημίπρωτοι,
παραγοντοποίηση κ.λπ.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία χρησιμοποιείται ευρύτατα

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία **χρησιμοποιείται** ευρύτατα
σήμερα στην **καθημερινότητα**

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία χρησιμοποιείται ευρύτατα σήμερα στην καθημερινότητα χωρίς να γίνεται αντιληπτό.



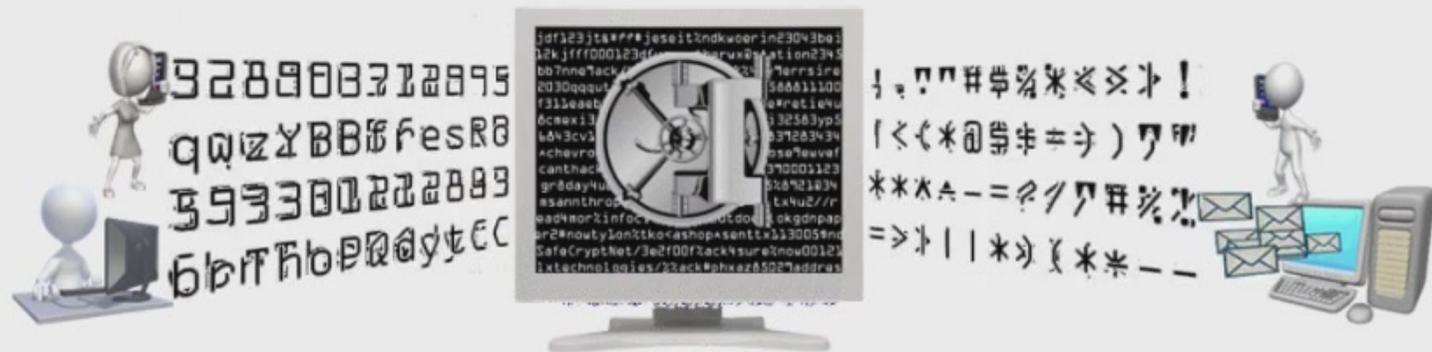
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία χρησιμοποιείται ευρύτατα σήμερα στην καθημερινότητα χωρίς να γίνεται αντιληπτό, σε ηλεκτρονικές συναλλαγές,



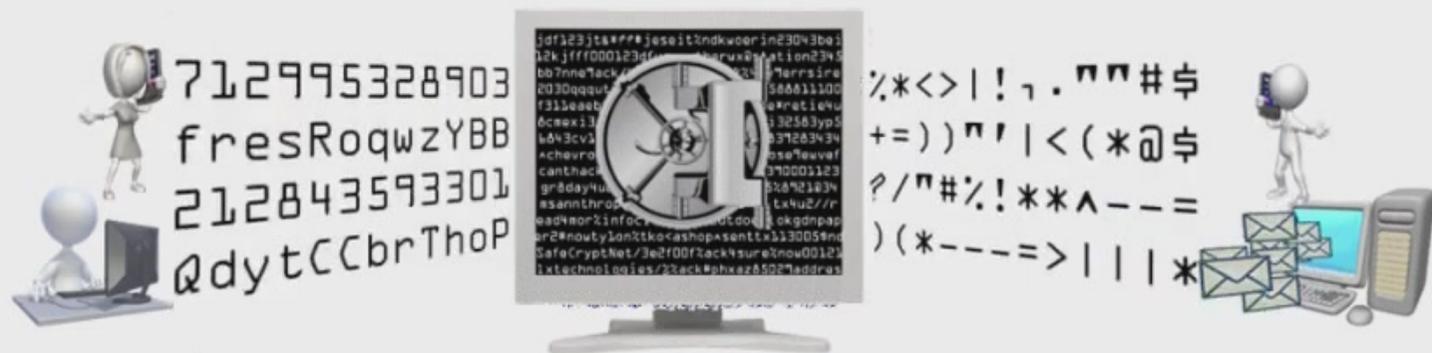
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία χρησιμοποιείται ευρύτατα σήμερα στην καθημερινότητα χωρίς να γίνεται αντιληπτό, σε ηλεκτρονικές συναλλαγές, κινητή τηλεφωνία αλλά και στα ασύρματα.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

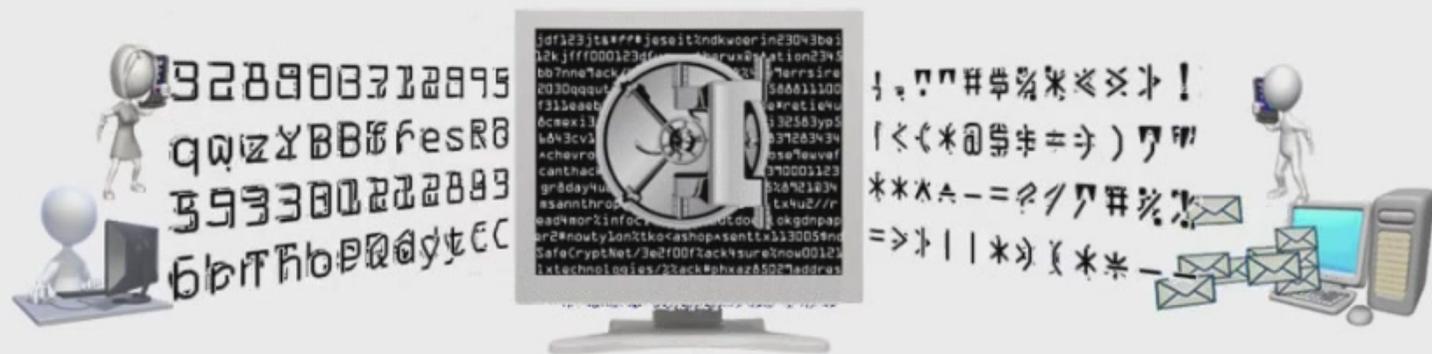
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία **χρησιμοποιείται** ευρύτατα σήμερα στην **καθημερινότητα** χωρίς να **γίνεται αντιληπτό**, σε **ηλεκτρονικές συναλλαγές**, **κινητή τηλεφωνία** αλλά και **στα ασύρματα δίκτυα (Wifi)**.



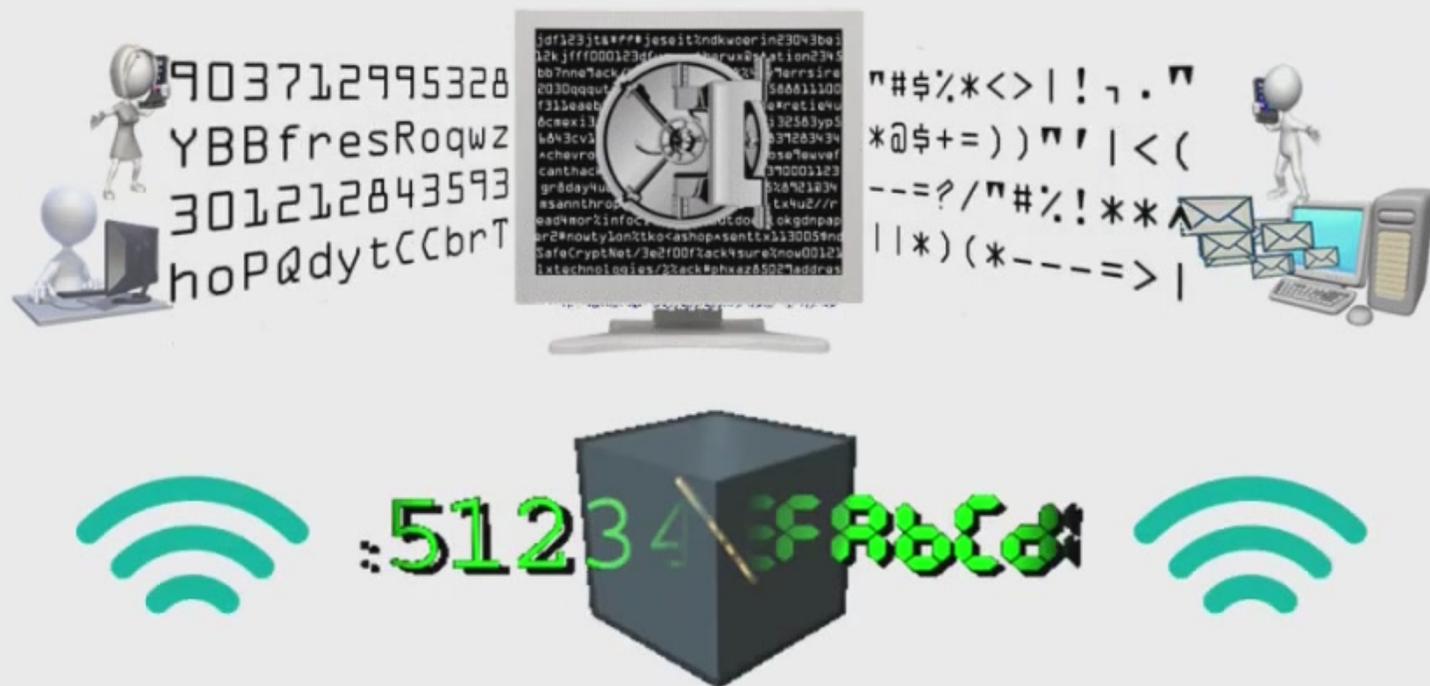
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία **χρησιμοποιείται** ευρύτατα σήμερα στην **καθημερινότητα** χωρίς να **γίνεται αντιληπτό**, σε **ηλεκτρονικές συναλλαγές**, **κινητή τηλεφωνία** αλλά και στα **ασύρματα δίκτυα (Wifi)**.



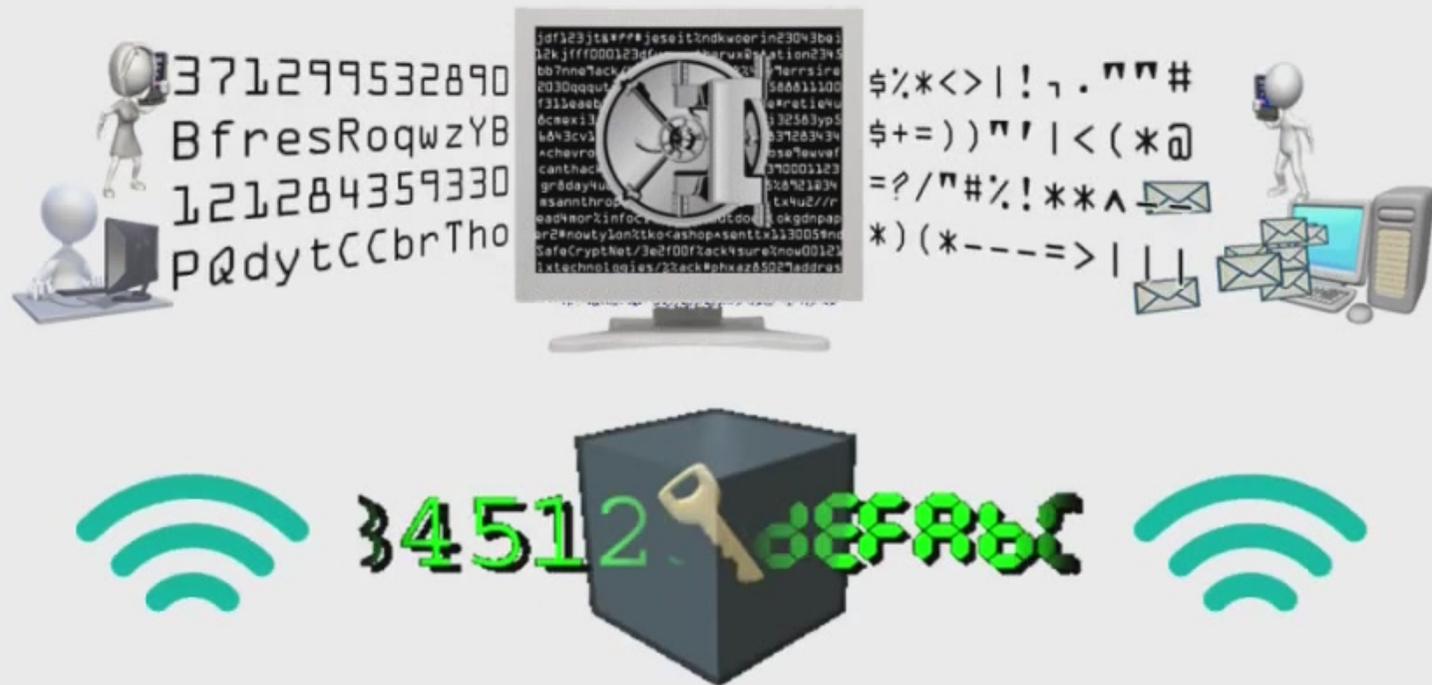
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία **χρησιμοποιείται** ευρύτατα σήμερα στην **καθημερινότητα** χωρίς να **γίνεται αντιληπτό**, σε **ηλεκτρονικές συναλλαγές**, **κινητή τηλεφωνία** αλλά και στα **ασύρματα δίκτυα (Wifi)**.



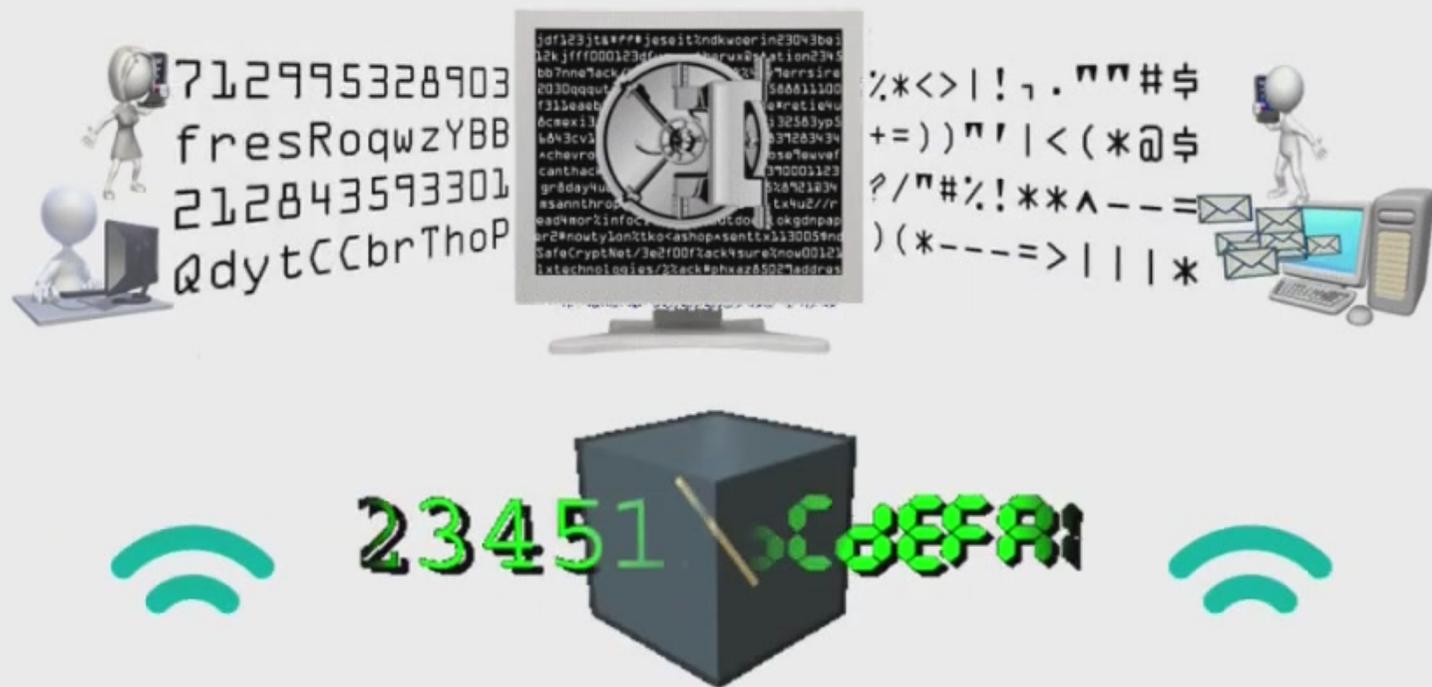
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία **χρησιμοποιείται** ευρύτατα σήμερα στην **καθημερινότητα** χωρίς να **γίνεται αντιληπτό**, σε **ηλεκτρονικές συναλλαγές**, **κινητή τηλεφωνία** αλλά και στα **ασύρματα δίκτυα (Wifi)**.



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Η κρυπτογραφία **χρησιμοποιείται** ευρύτατα σήμερα στην **καθημερινότητα** χωρίς να **γίνεται αντιληπτό**, σε **ηλεκτρονικές συναλλαγές**, **κινητή τηλεφωνία** αλλά και στα **ασύρματα δίκτυα (Wifi)**.



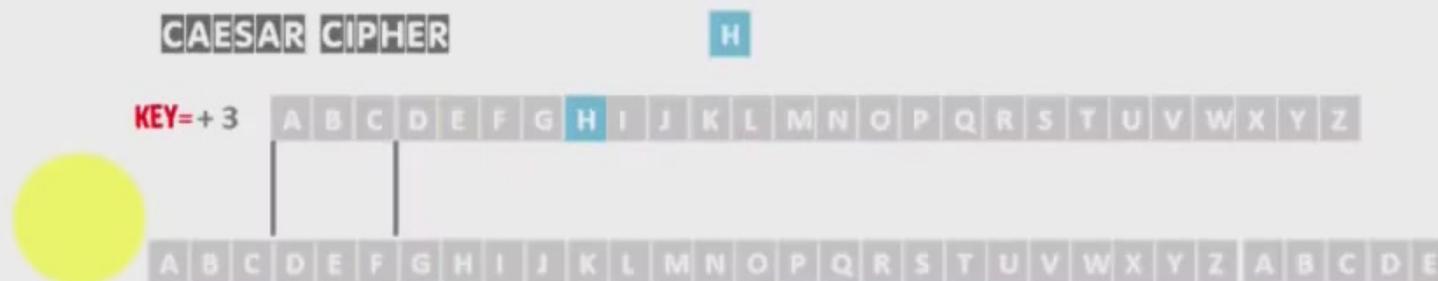
ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)



CAESAR CIPHER

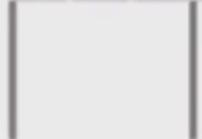
H E

KEY=+3

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

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 A B C D E

K



CAESAR CIPHER

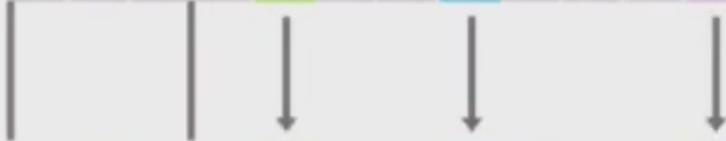
H E L

KEY=+3

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

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 A B C D E

K H O

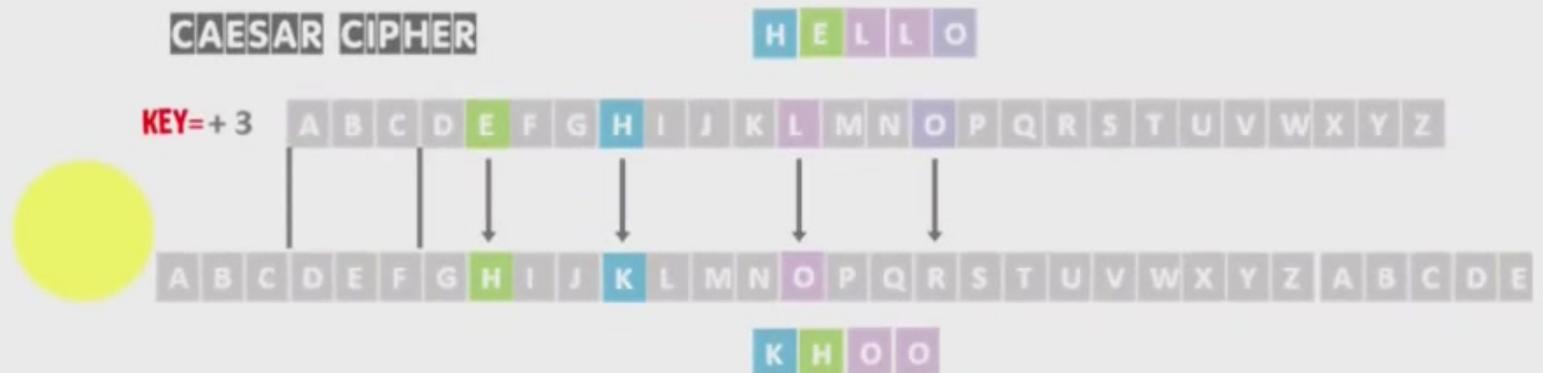


Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

Ασφάλεια Λογισμικού

Κρυπτογραφία (Cryptography)



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

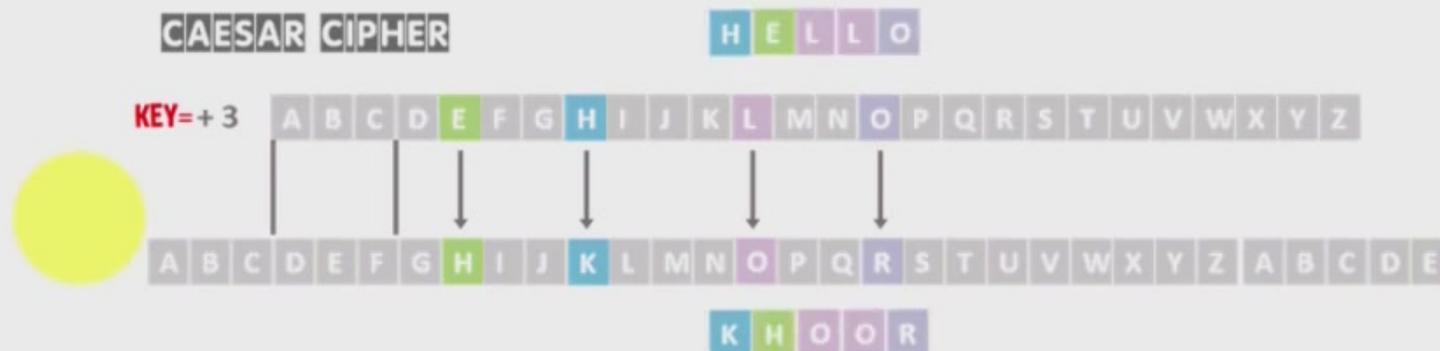
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που θέλουν να πετύχουν



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

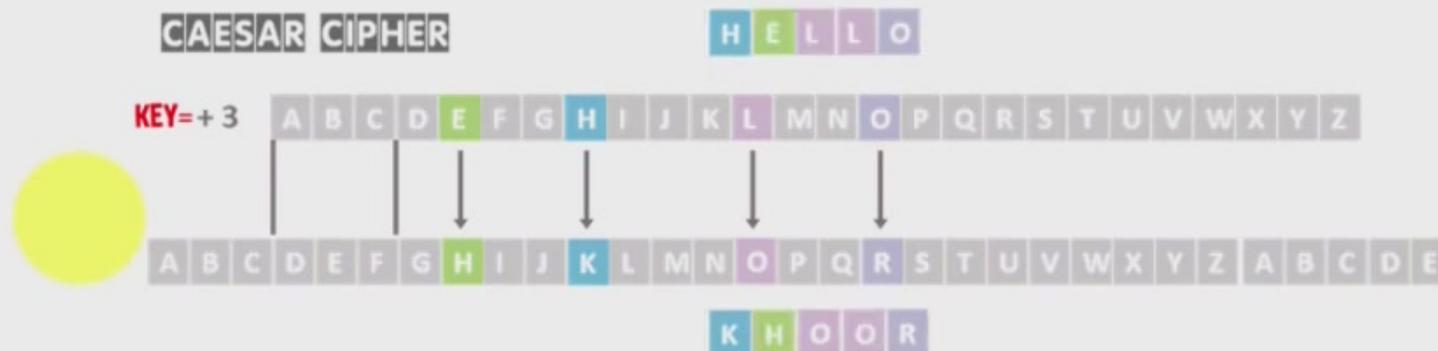
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν**
οι **αλγόριθμοι κρυπτογράφησης**
μπορεί



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

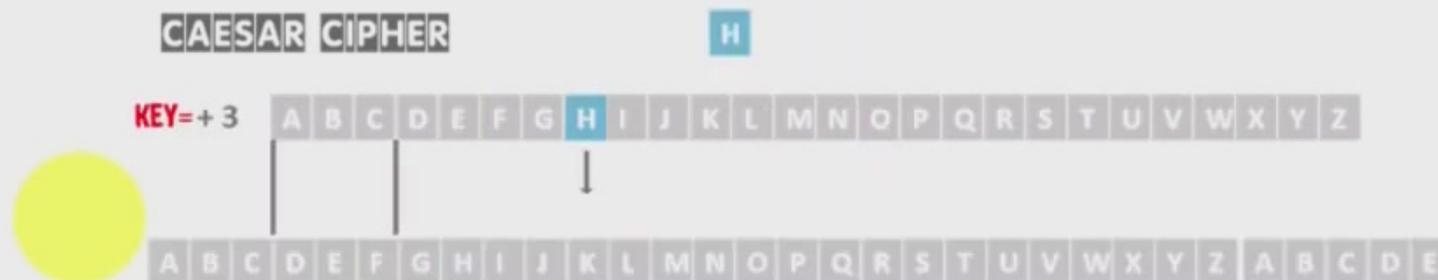
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν**
οι **αλγόριθμοι κρυπτογράφησης**
μπορεί να περιγραφεί ως εξής:
έστω πως υπάρχουν **δύο φίλοι**.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

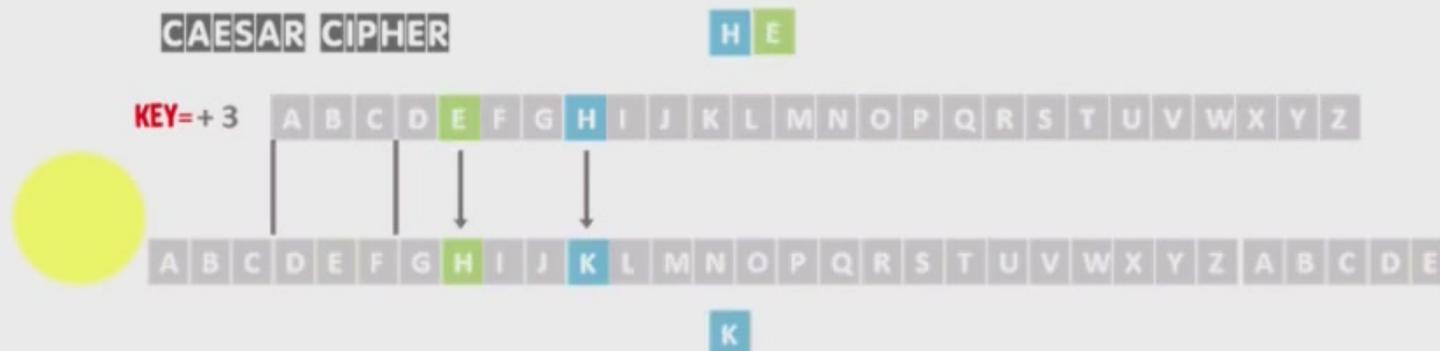
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν**
οι **αλγόριθμοι κρυπτογράφησης**
μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**,
ο Άκης και η **Βούλα**,



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

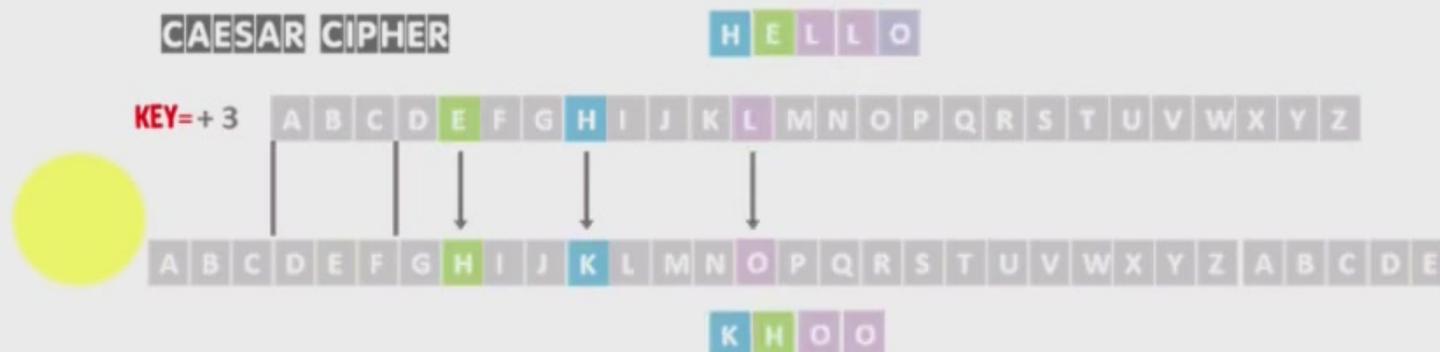
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να περιγραφεί ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια**



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

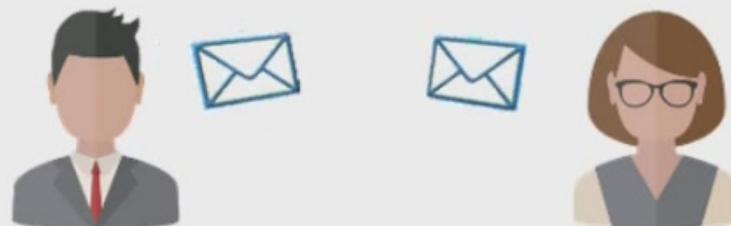
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

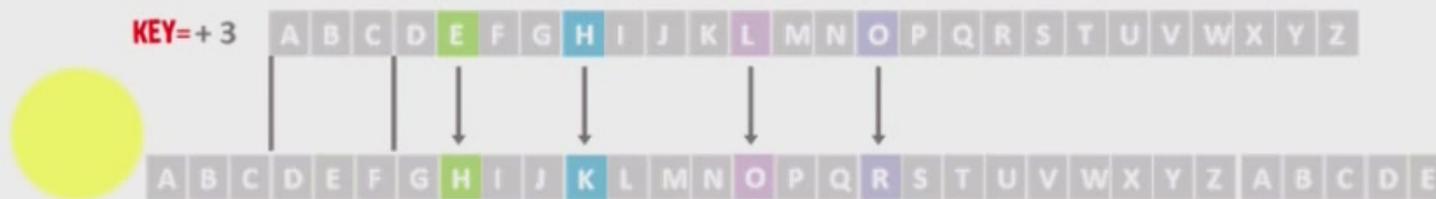
5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να περιγραφεί ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν μηνύματα με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν).



CAESAR CIPHER

KEY=+3



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

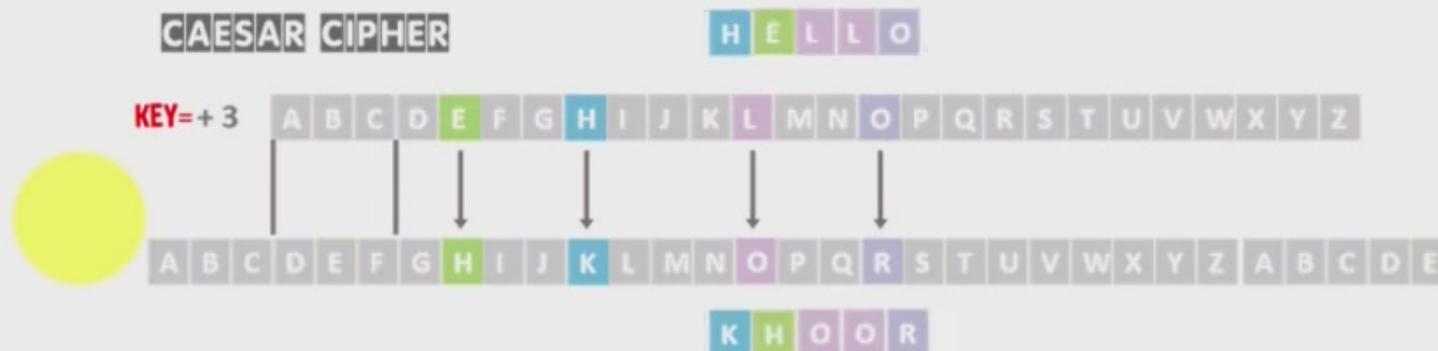
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να περιγραφεί ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν).
Ο Άκης, αφού ετοιμάσει το μήνυμά του,



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

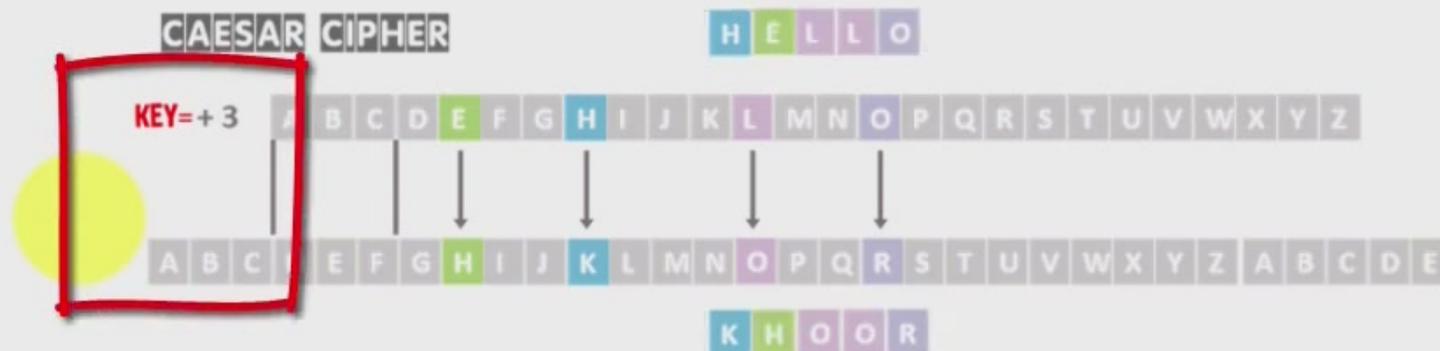
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν).
Ο **Άκης**, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει** με **κάποιο κλειδί**



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

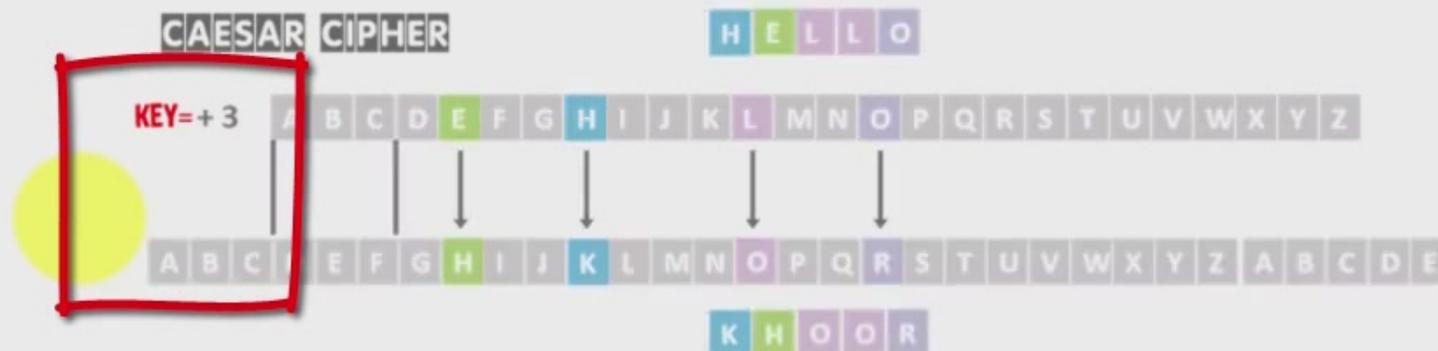
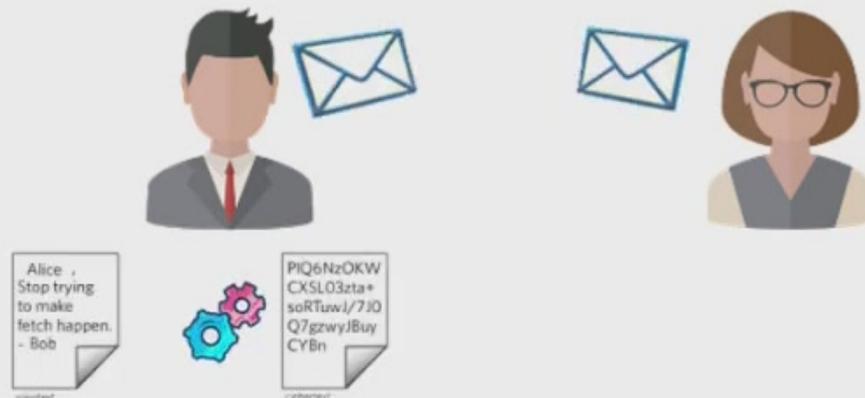
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να περιγραφεί ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι θέλουν να **ανταλλάξουν** μηνύματα με **ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει με κάτποιο κλειδί** σε **μη αναγνώσιμη** από άλλους μ



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

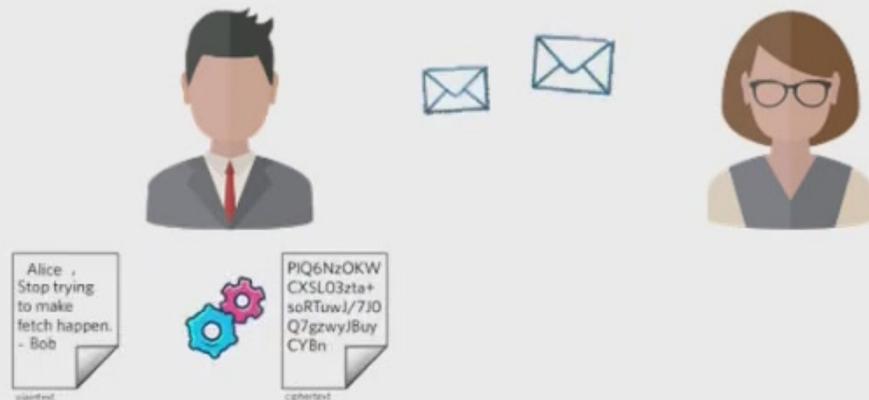
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει** με **κάποιο κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα



CAESAR CIPHER

KEY=+3



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

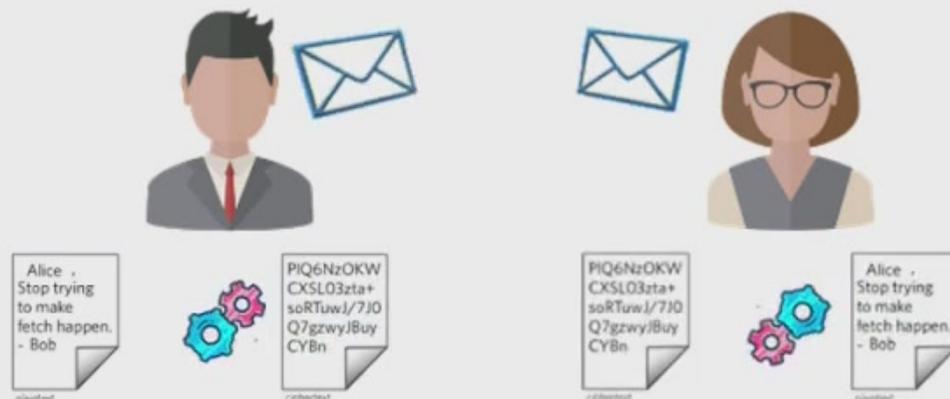
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

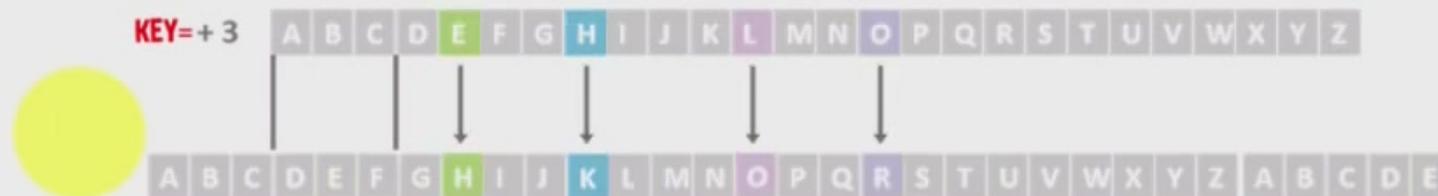
5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει** με **κάποιο κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή **έτσι ώστε μόνο η Βούλα** θα μπορεί να το **ξεκλειδώσει**



CAESAR CIPHER



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

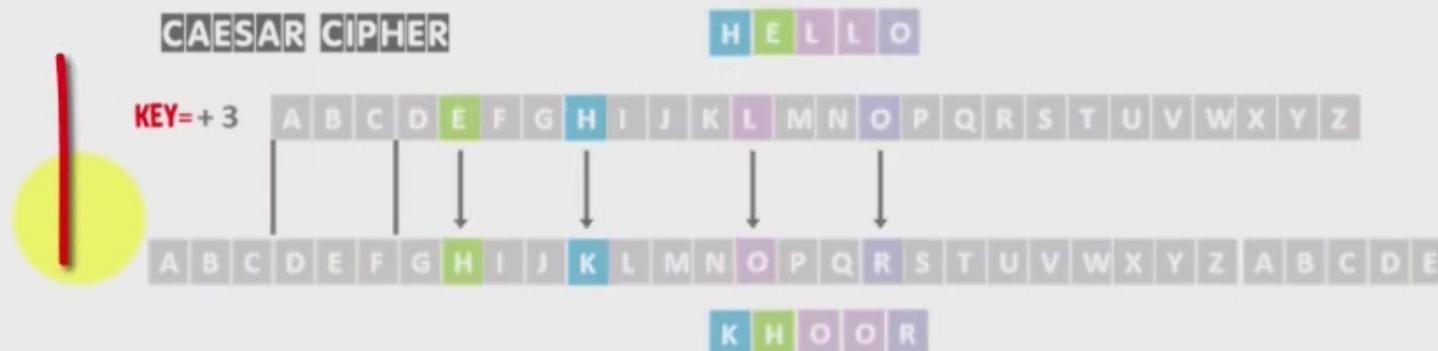
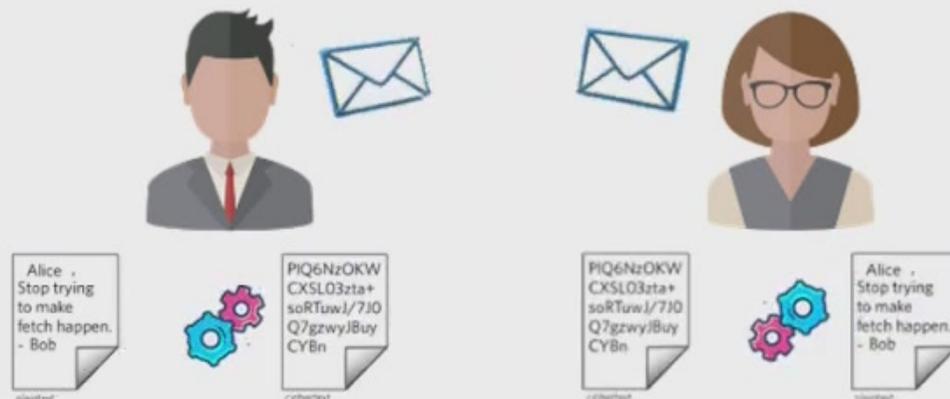
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι θέλουν να **ανταλλάξουν** μηνύματα με **ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει** με **κάποιο κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να το **ξεκλειδώσει**



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

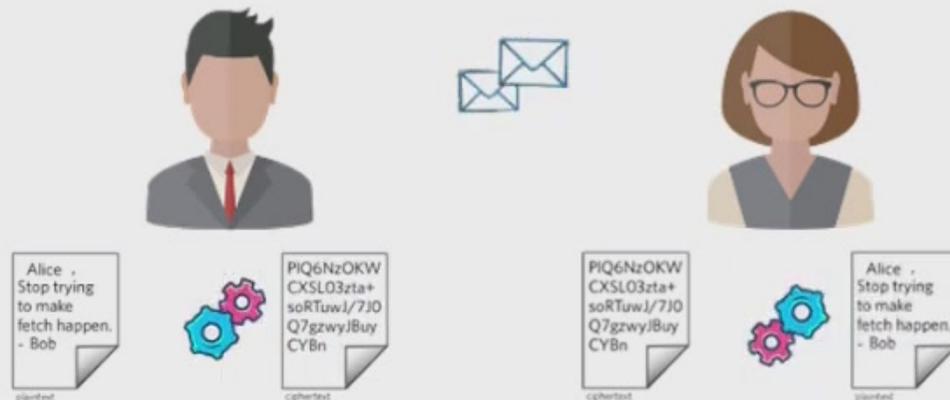
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα **το μετατρέψει** με **κάποιο κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να **διαβάσει το περιεχόμενό του**.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

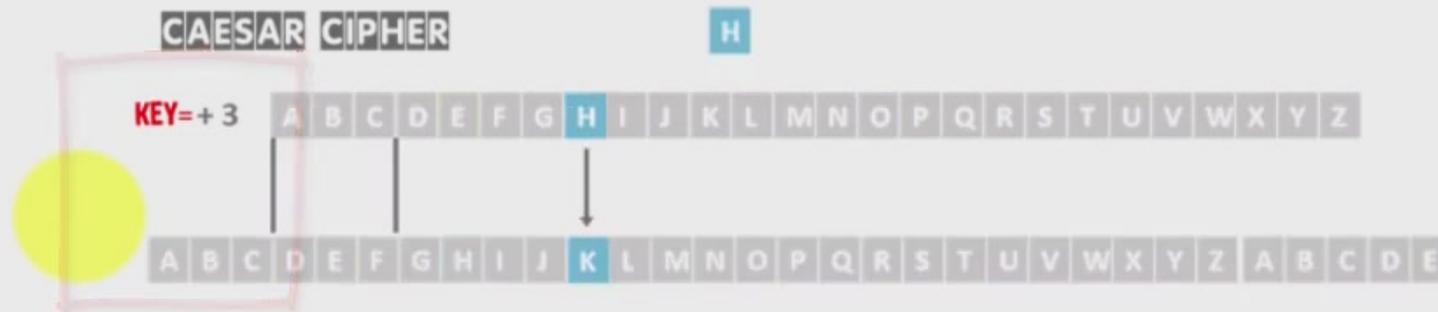
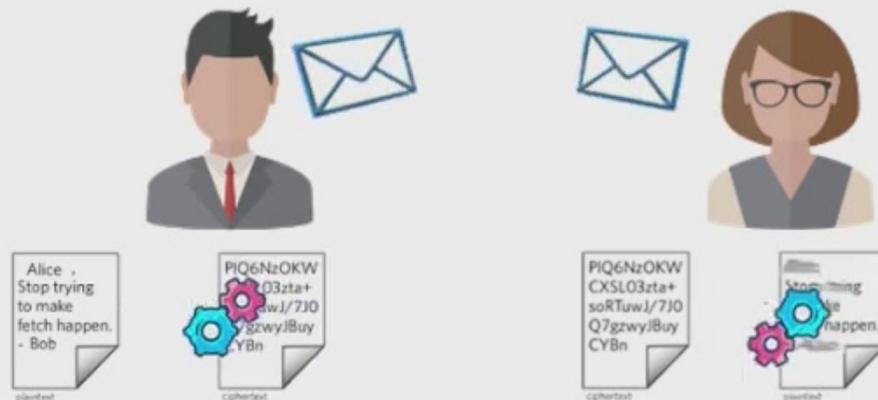
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει** με **κάποιο κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να **διαβάσει το περιεχόμενό του**.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν**

οι **αλγόριθμοι κρυπτογράφησης**

μπορεί να **περιγραφεί** ως εξής:

έστω πως υπάρχουν **δύο φίλοι**,

ο **Άκης** και η **Βούλα**,

οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια**

(μόνο αυτοί να μπορούν να τα διαβάσουν).

Ο Άκης, αφού ετοιμάσει το μήνυμά του,

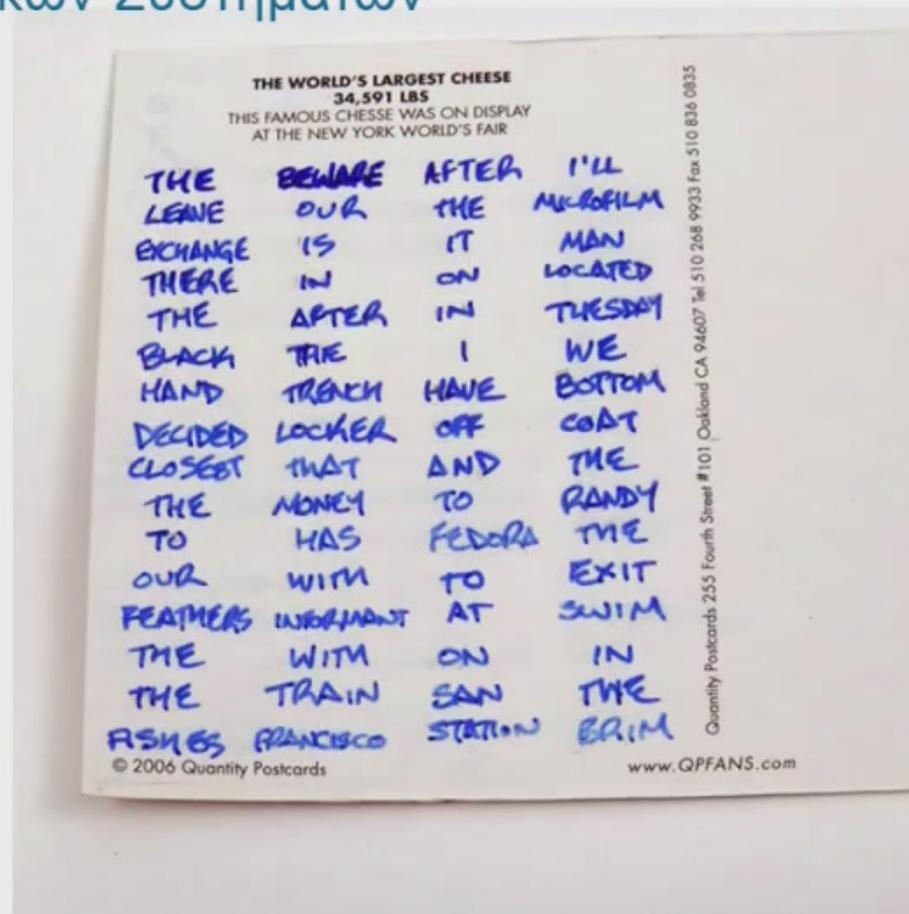
θα **το μετατρέψει με κάποιον κλειδί**

σε **μη αναγνώσιμη** από άλλους μορφή

έτσι ώστε μόνο η Βούλα

θα μπορεί να **το ξεκλειδώσει**

και να διαβάσει το περιεχόμενό του.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν**

οι **αλγόριθμοι κρυπτογράφησης**

μπορεί να **περιγραφεί** ως εξής:

έστω πως υπάρχουν **δύο φίλοι**,

ο **Άκης** και η **Βούλα**,

οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια**

(μόνο αυτοί να μπορούν να τα διαβάσουν).

Ο Άκης, αφού ετοιμάσει το μήνυμά του,

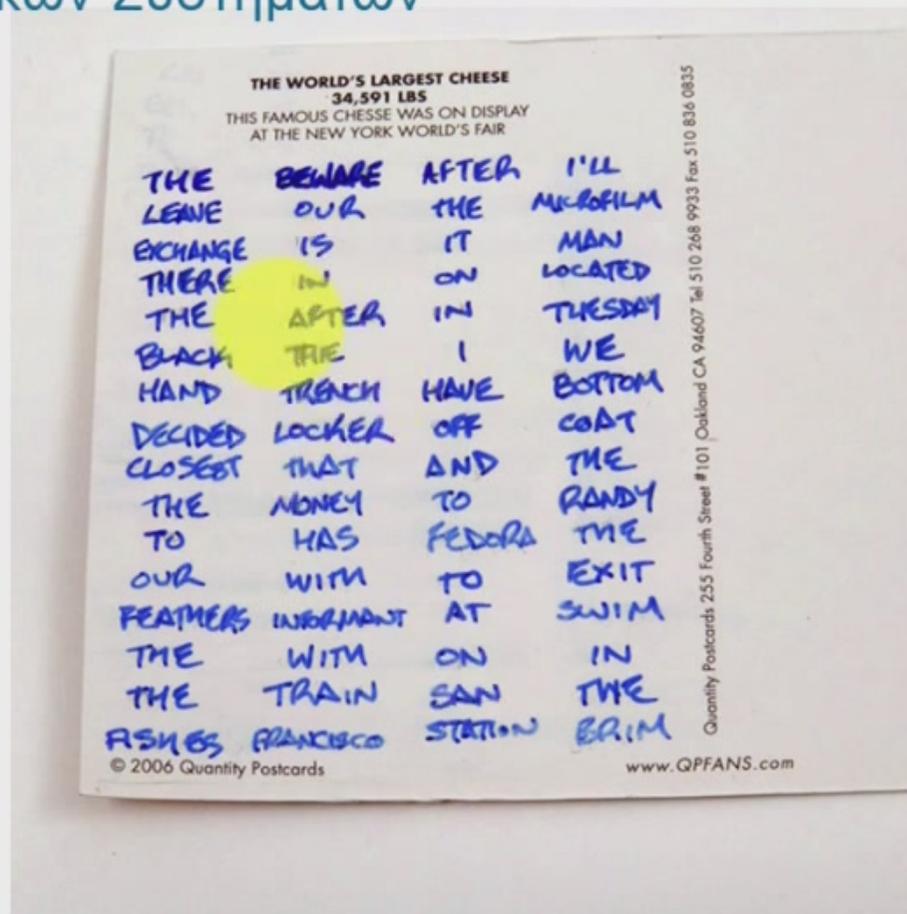
θα **το μετατρέψει με κάποιον κλειδί**

σε **μη αναγνώσιμη** από άλλους μορφή

έτσι ώστε μόνο η Βούλα

θα μπορεί να **το ξεκλειδώσει**

και να διαβάσει το περιεχόμενό του.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

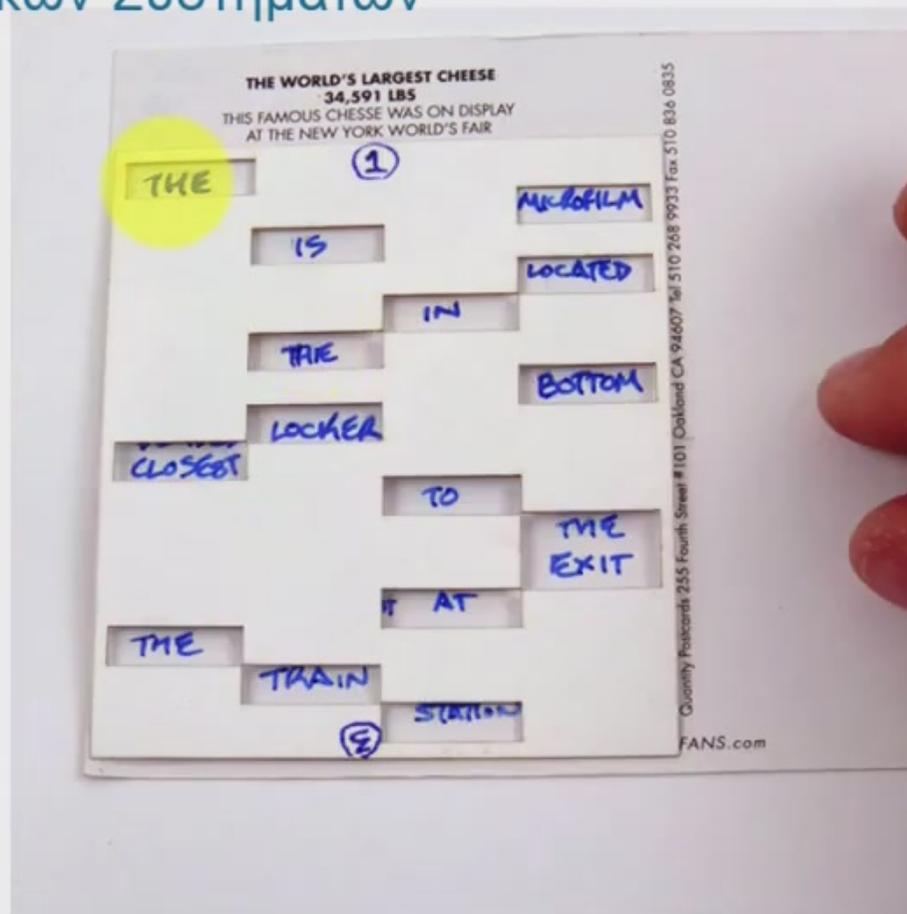
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει** με **κάποιο κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να διαβάσει το περιεχόμενό του.



①

THE

MICROFILM

IS

LOCATED

IN

THE

BOTTOM

LOCKER

CLOSEST

TO

THE
EXIT

IT AT

THE

TRAIN

STATION

②

THIS FAMOUS STREET
AT THE NEW YORK WORLD'S FAIR

2

I'LL

LEAVE

IT

THERE

AFTER

I

HAND

OFF

THE

MONEY

TO
OUR

INFORMATION

IN

SAN

FRANCISCO

4



Quantity Postcards 255 Fourth Street #101 Oakland CA 94607 Tel 510 268 9933 Fax 510 8

FANS.com

THIS FAMOUS STREET
AT THE NEW YORK WORLD'S FAIR

②

I'LL

LEAVE

IT

THERE

AFTER

I

HAND

OFF

THE

MONEY

TO
OUR

INTERMAN

IN

SAN

FRANCISCO

④



Quantity Postcards 255 Fourth Street #101 Oakland CA 94607 Tel 510 268 9933 Fax 510 8

FANS.com

THIS FAMOUS SERIES
AT THE NEW YORK WORLD'S FAIR

②

I'LL

LEAVE

IT

THERE

AFTER

I

HAND

OFF

THE

MONEY

TO
OUR

INTERMAN

IN

FRANCISCO

④

Quantity Postcards 255 Fourth Street #101 Oakland CA 94607 Tel 510 268 9933 Fax 510 8



FANS.com

THIS FAMOUS STREET
AT THE NEW YORK WORLD'S FAIR

Beware

(3)

THE

MAN

IN

THE
BLACK

TRENCH

COAT

AND

THE

FEDORA

WITH

FEATHERS

ON

THE

BRIM

(T)

Quantity Postcards 255 Fourth Street #101 Oakland CA 94607 Tel 510 268 9933 Fax 510 8

FANS.com



THIS FAMOUS SERIES
AT THE NEW YORK WORLD'S FAIR

BEWARE

③

THE

MAN

IN

THE
BLACK

TRENCH

COAT

AND

THE

FEDORA

WITH

FEATHERS

ON

THE

BRIM

Ⓟ

Quantity Postcards 255 Fourth Street #101 Oakland CA 94607 Tel 510 268 9933 Fax 510 8

FANS.com



THIS FAMOUS...
AT THE NEW YORK WORLD'S FAIR

④

AFTER

OUR

EXCHANGE

ON

TUESDAY

WE

HAVE

DECIDED

THAT

RANDY

HAS

TO

SWIM

WITH

THE

ASHES

⑦



Quantity Postcards 255 Fourth Street #101 Oakland CA 94607 Tel 510 268 9933 Fax 510 8

FANS.com

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

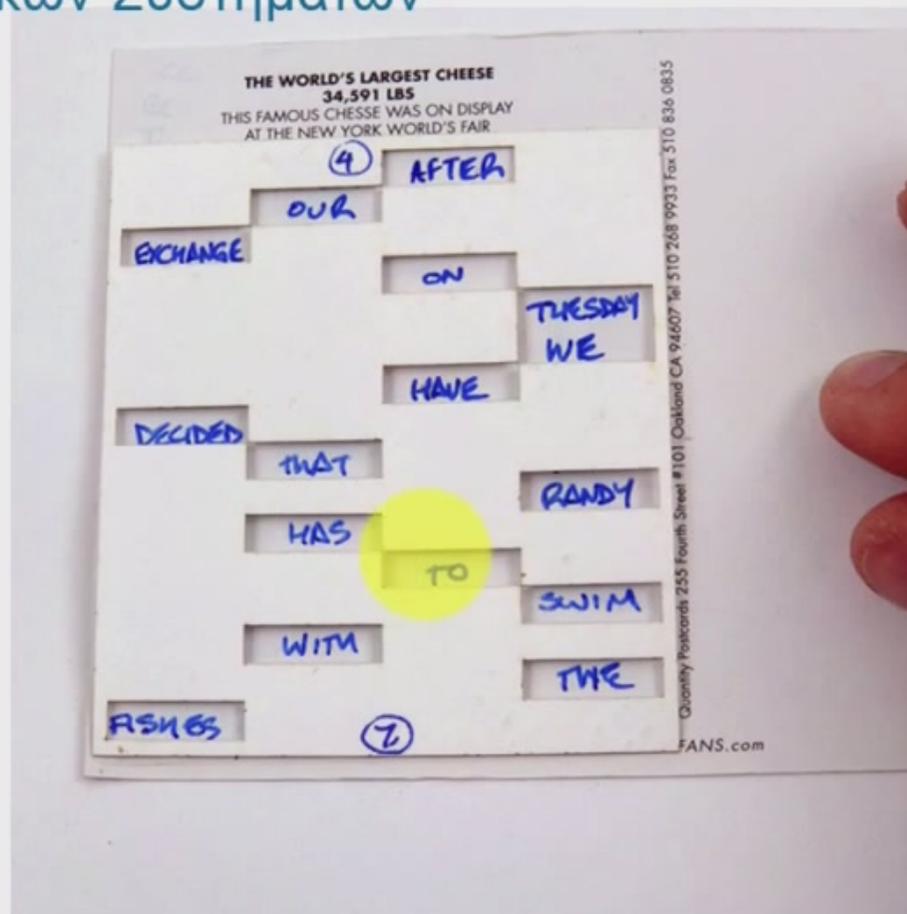
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει με κάποιον κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να διαβάσει το περιεχόμενό του.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

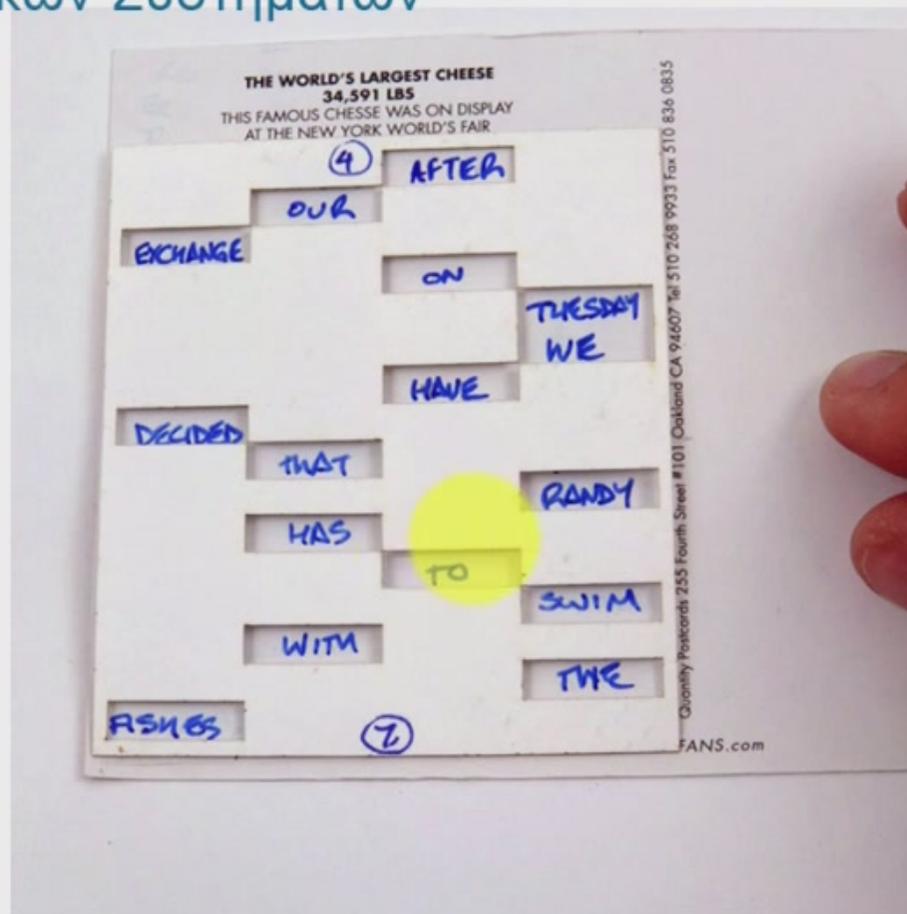
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει με κάποιον κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να διαβάσει το περιεχόμενό του.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν**

οι **αλγόριθμοι κρυπτογράφησης**

μπορεί να **περιγραφεί** ως εξής:

έστω πως υπάρχουν **δύο φίλοι**,

ο **Άκης** και η **Βούλα**,

οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια**
(μόνο αυτοί να μπορούν να τα διαβάσουν).

Ο Άκης, αφού ετοιμάσει το μήνυμά του,

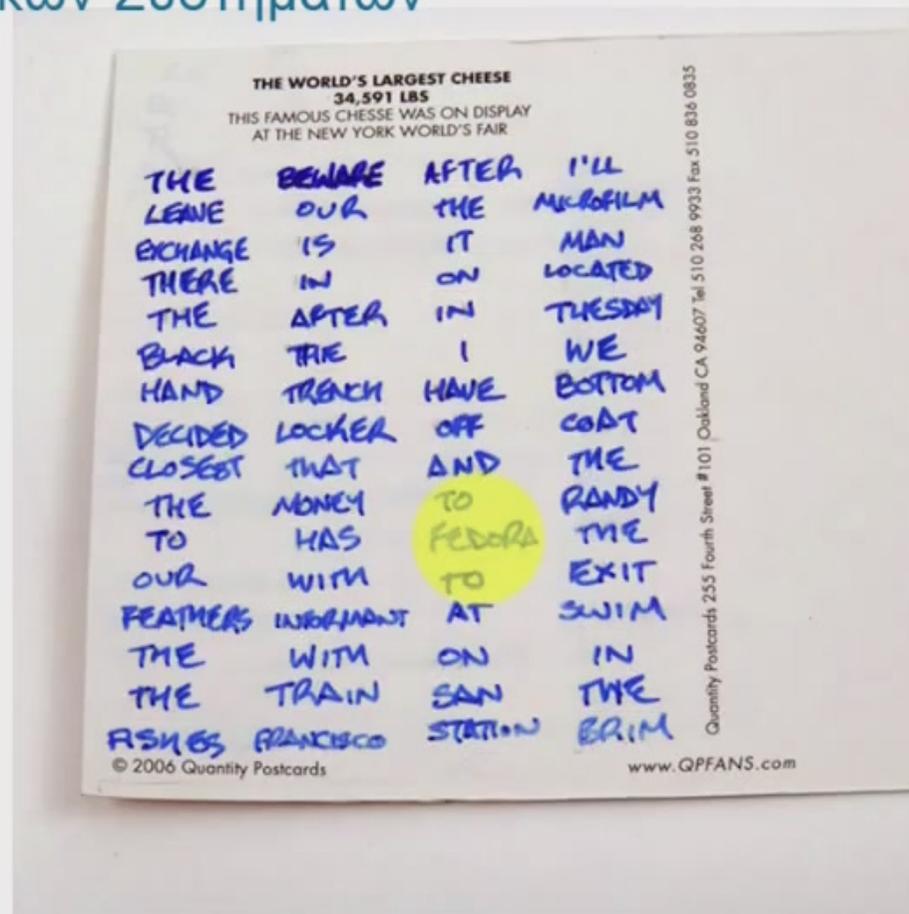
θα **το μετατρέψει με κάποιον κλειδί**

σε **μη αναγνώσιμη** από άλλους μορφή

έτσι ώστε μόνο η Βούλα

θα μπορεί να **το ξεκλειδώσει**

και να διαβάσει το περιεχόμενό του.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν**

οι **αλγόριθμοι κρυπτογράφησης**

μπορεί να **περιγραφεί** ως εξής:

έστω πως υπάρχουν **δύο φίλοι**,

ο **Άκης** και η **Βούλα**,

οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια**

(μόνο αυτοί να μπορούν να τα διαβάσουν).

Ο Άκης, αφού ετοιμάσει το μήνυμά του,

θα το **μετατρέψει** με **κάποιο κλειδί**

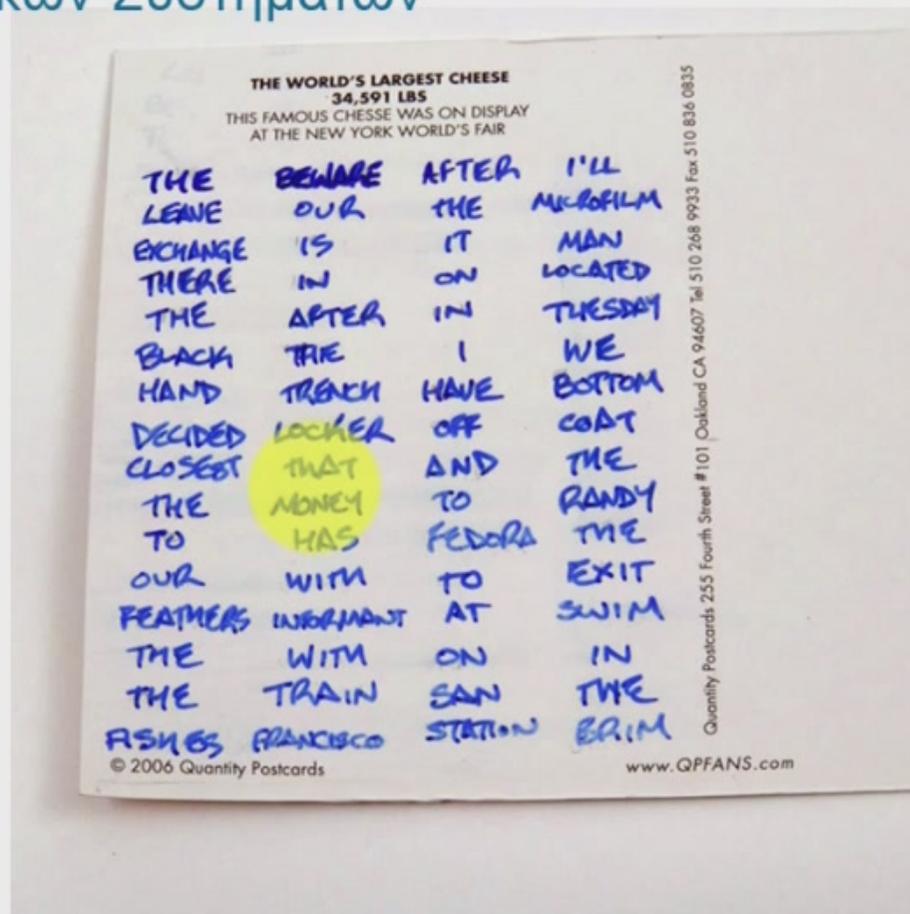
σε **μη αναγνώσιμη** από άλλους μορφή

έτσι ώστε μόνο η Βούλα

θα μπορεί να **το ξεκλειδώσει**

και να διαβάσει το περιεχόμενό του.

HELLO



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

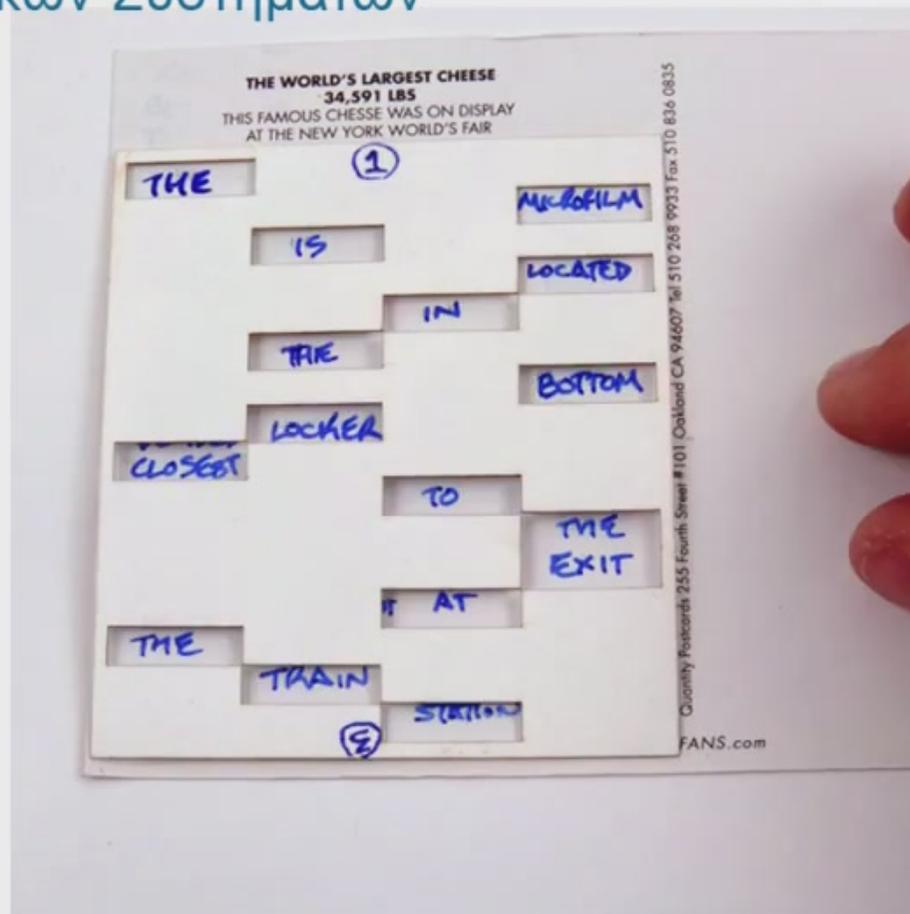
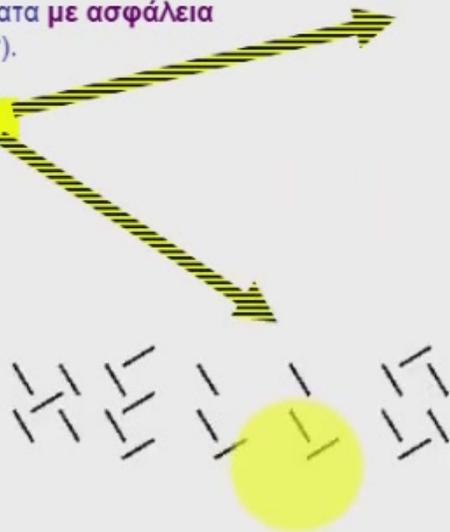
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να περιγραφεί ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει με κάποιον κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να διαβάσει το περιεχόμενό του.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

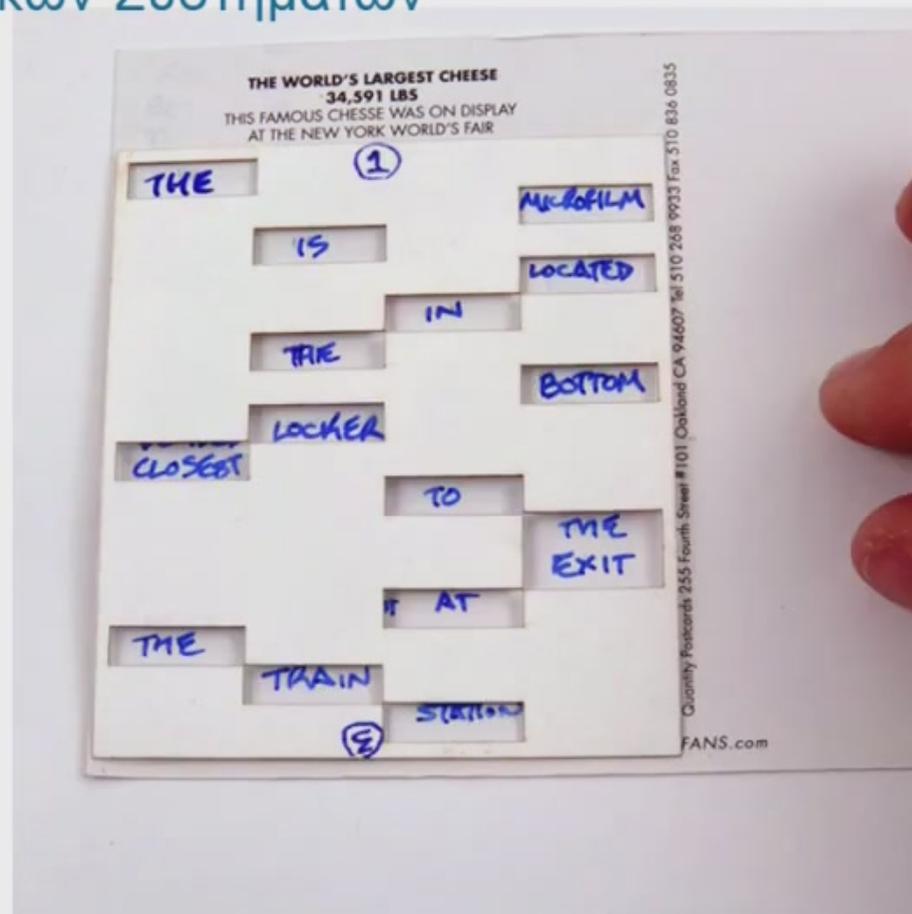
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει με κάποιον κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να διαβάσει το περιεχόμενό του.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

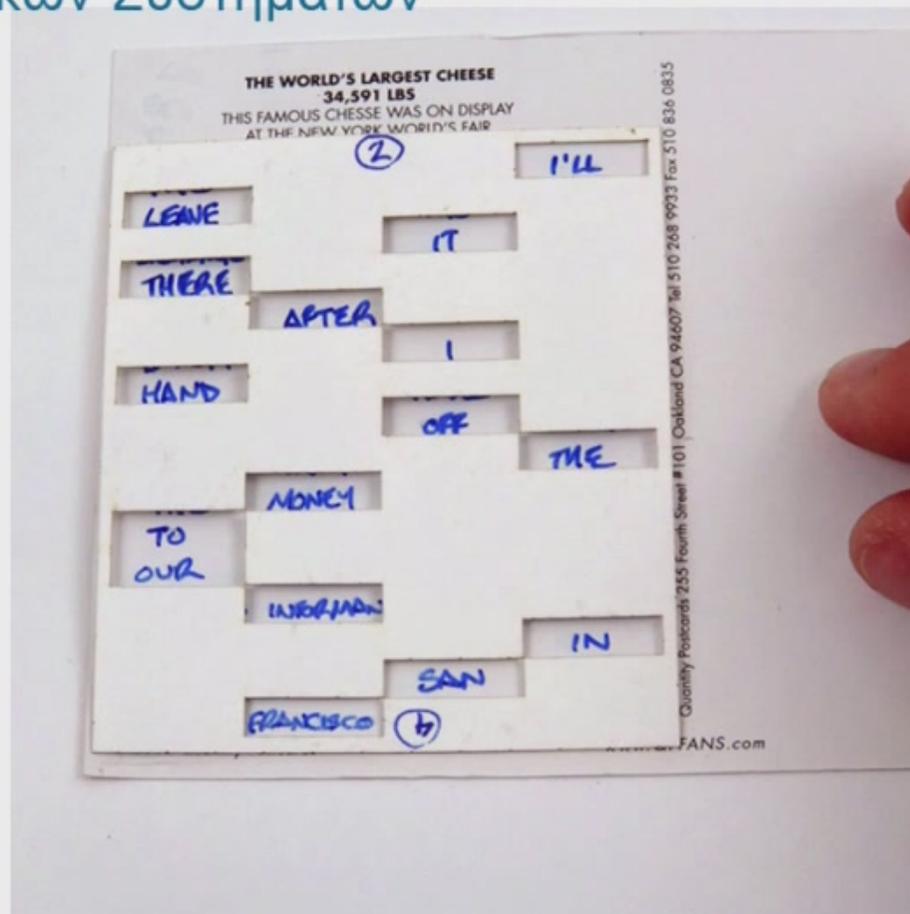
Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει με κάποιον κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να διαβάσει το περιεχόμενό του.

H E L L O



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

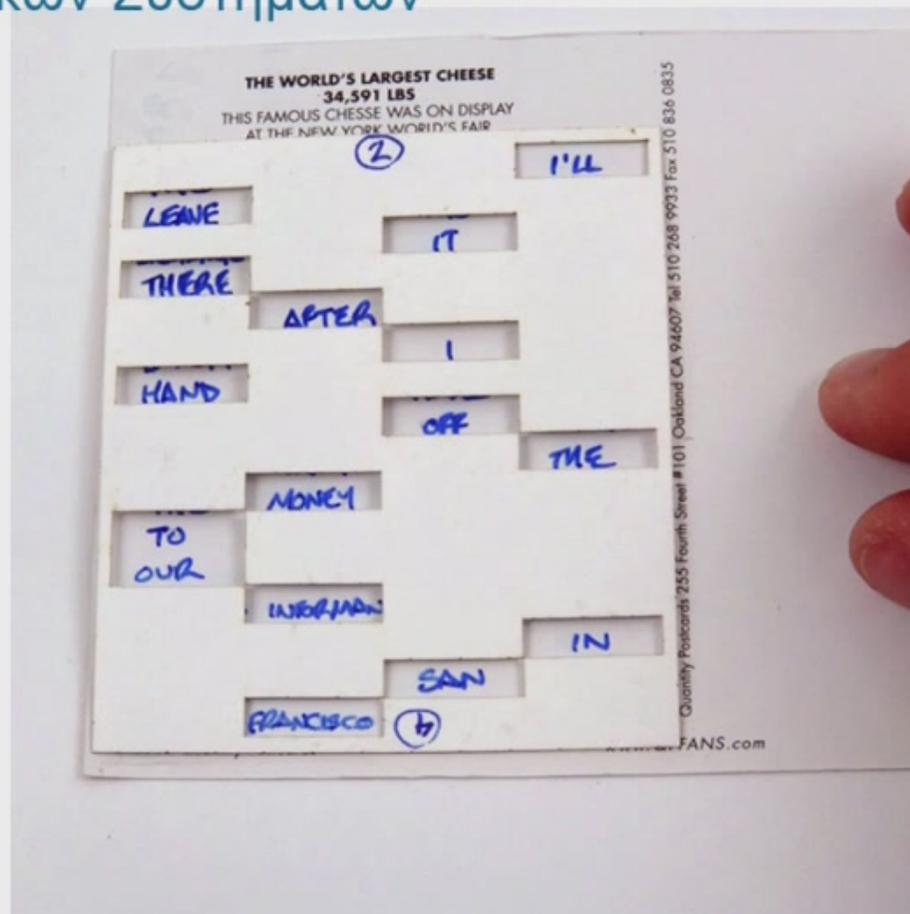
Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει με κάποιον κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να διαβάσει το περιεχόμενό του.

H E L L O



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

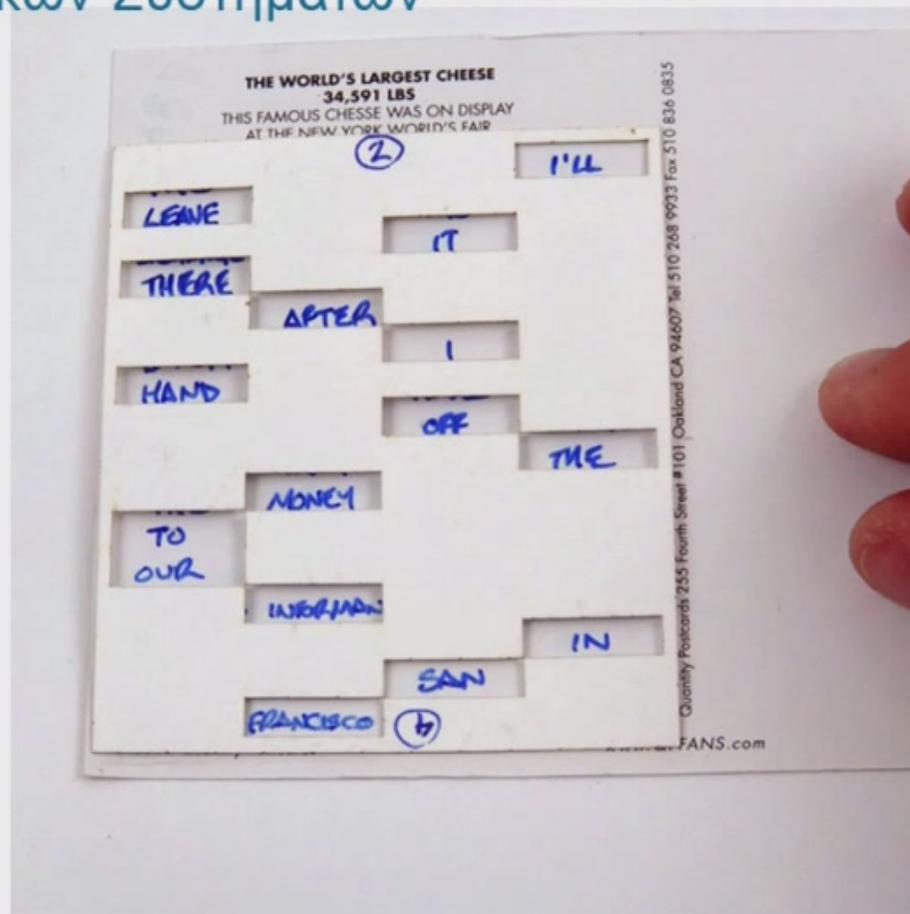
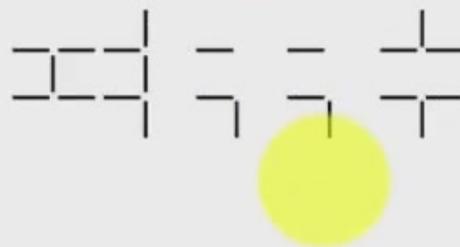
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Σε γενικές γραμμές αυτό που **θέλουν να πετύχουν** οι **αλγόριθμοι κρυπτογράφησης** μπορεί να **περιγραφεί** ως εξής:
έστω πως υπάρχουν **δύο φίλοι**, ο **Άκης** και η **Βούλα**, οι οποίοι **θέλουν να ανταλλάξουν** μηνύματα **με ασφάλεια** (μόνο αυτοί να μπορούν να τα διαβάσουν). Ο Άκης, αφού ετοιμάσει το μήνυμά του, θα το **μετατρέψει με κάποιον κλειδί** σε **μη αναγνώσιμη** από άλλους μορφή έτσι ώστε μόνο η Βούλα θα μπορεί να **το ξεκλειδώσει** και να διαβάσει το περιεχόμενό του.



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμ

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο Κ

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

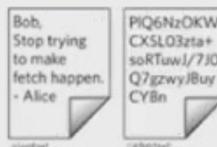
5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption):**

Η διαδικασία μετασχηματισμού του μηνύματος



phy)

είναι η παρακάτω:

ηνύματος
ναγνώσιμο

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuY
CYBn

ciphertext

Άλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

Ασφάλεια Λογισμικού

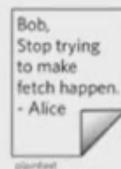
Κρυπτογραφία (Cryptography)

ήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

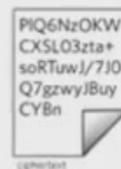
Κρυπτογράφηση (Encryption):

Η διαδικασία μετασχηματισμού του μηνύματος
από το αρχικό μήνυμα στο τελικό μη αναγνώσιμο

Bob,
Stop trying
to make
fetch happen.
- Alice



PIQ6NzOKW
CXSL03zta+
soRTUwJ/7J0
Q7gzwyJBuy
CYBn



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η διαδικασία μετασχηματισμού του μηνύματος από το αρχικό μήνυμα στο τελικό μη αναγνώσιμο
- ο **Αποκρυπτογράφηση (Decryption)**:

Bob,
Stop trying
to make
fetch happen.
- Alice

PIQ6NzOKW
CXSL03zta+
soRTuwj/7J0
Q7gzwyjBuy
CYBn

PIQ6NzOKW
CXSL03zta+
soRTuwj/7J0
Q7gzwyjBuy
CYBn

Bob,
Stop trying
to make
fetch happen.
- Alice

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος**
από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της κρυπτογράφησης

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuY
CYBn

ciphertext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuY
CYBn

ciphertext

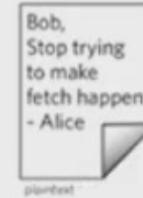
Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

5.3.4 Κρυπτογραφία (Cryptography)

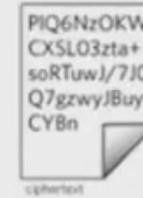
Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος**
από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**
- ο **Απλό κείμενο (Plaintext)**:



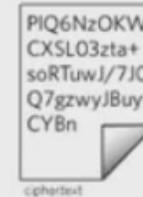
Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext



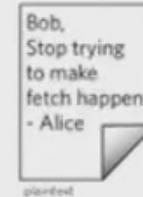
PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext



PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext



Bob,
Stop trying
to make
fetch happen.
- Alice

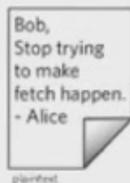
plaintext

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος**
από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**
- ο **Απλό κείμενο (Plaintext)**:
το αρχικό μήνυμα



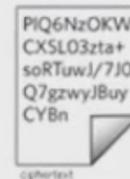
Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext



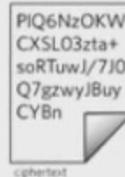
Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext



PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext



PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext



Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος**
από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**
- ο **Απλό κείμενο (Plaintext)**:
το **αρχικό μήνυμα**
- ο **Αλγόριθμος κρυπτογράφησης (Cipher)**:



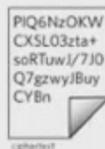
Bob,
Stop trying
to make
fetch happen.
- Alice



Bob,
Stop trying
to make
fetch happen.
- Alice



PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyjBuy
CY8n



PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyjBuy
CY8n



Bob,
Stop trying
to make
fetch happen.
- Alice

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**
- ο **Απλό κείμενο (Plaintext)**:
το **αρχικό μήνυμα**
- ο **Αλγόριθμος κρυπτογράφησης (Cipher)**:
ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα

Bob,
Stop trying
to make
fetch happen.
- Alice

PIQ6NzOKW
CXSL03zta+
soRTuwI/7J0
Q7gzwyJBuy
CYBn

PIQ6NzOKW
CXSL03zta+
soRTuwI/7J0
Q7gzwyJBuy
CYBn

Stop trying
to n
fet
- Alice

Bob,
Stop trying
to make
fetch happen.
- Alice

- Alice fetch happen. to make Stop trying Bob,



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

- ο **Αποκρυπτογράφηση (Decryption)**:

η **αντίστροφη διαδικασία** της **κρυπτογράφησης**

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)** :

ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα** σε **μη αναγνώσιμο**

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- Alice fetch happen. to make Stop trying Bob,



Κεφάλαιο 5ο

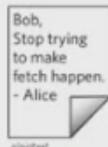
Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**
- ο **Απλό κείμενο (Plaintext)**:
το **αρχικό μήνυμα**
- ο **Αλγόριθμος κρυπτογράφησης (Cipher)** :
ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί το αρχικό μήνυμα σε μη αναγνώσιμο**
- ο **Κρυπτογράφημα (ciphertext)**:



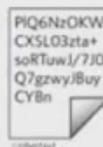
Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext



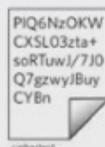
Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext



PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

ciphertext



PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

ciphertext



Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- Alice fetch happen. to make Stop trying Bob,



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**
- ο **Απλό κείμενο (Plaintext)**:
το **αρχικό μήνυμα**
- ο **Αλγόριθμος κρυπτογράφησης (Cipher)** :
ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**
- ο **Κρυπτογράφημα (ciphertext)**:
το **τελικό μη αναγνώσιμο μήνυμα**

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyjBuy
CYBn

ciphertext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyjBuy
CYBn

ciphertext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext



CYBn Q7gzwyjBuy soRTuwJ/7J0 CXSL03zta+ PIQ6NzOKW

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

- ο **Αποκρυπτογράφηση (Decryption)**:

η **αντίστροφη διαδικασία** της **κρυπτογράφησης**

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)** :

ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**

- ο **Κρυπτογράφημα (ciphertext)**:

το τελικό μη αναγνώσιμο μήνυμα

- ο **Κλειδί (key)**:

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7JO
Q7gzwyJBuy
CYBn

ciphertext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7JO
Q7gzwyJBuy
CYBn

ciphertext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- Alice fetch happen. to make Stop trying Bob,



PIQ6NzOKW
CXSL03zta+
soRTuwJ/7JO
Q7gzwyJBuy
CYBn

ciphertext

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

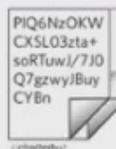


Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- ο **Αποκρυπτογράφηση (Decryption)**:

η **αντίστροφη διαδικασία** της **κρυπτογράφησης**



PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**



Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- Alice fetch happen. to make Stop trying Bob,

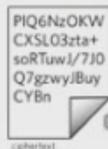
- ο **Αλγόριθμος κρυπτογράφησης (Cipher)** :

ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**



- ο **Κρυπτογράφημα (ciphertext)**:

το τελικό μη αναγνώσιμο μήνυμα



PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext

00110100101000011100100100011101010000111111111001010111

Διαφορετικοί συν

- ο **Κλειδί (key)**:

είναι μια **σειρά αρκετών bit**

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**
- ο **Απλό κείμενο (Plaintext)**:
το **αρχικό μήνυμα**
- ο **Αλγόριθμος κρυπτογράφησης (Cipher)** :
ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**
- ο **Κρυπτογράφημα (ciphertext)**:
το τελικό μη αναγνώσιμο μήνυμα
- ο **Κλειδί (key)**:
είναι μια **σειρά αρκετών bit**
που χρησιμοποιείται ως είσοδος στη

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

ciphertext

PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

ciphertext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- Alice fetch happen. to make Stop trying Bob,



PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

ciphertext

0011010010100001110010010001110101000011111111100101011

Διαφορετικοί συνδυασμοί

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- ο **Αποκρυπτογράφηση (Decryption)**:

η **αντίστροφη διαδικασία** της **κρυπτογράφησης**

PIQ6NzOKW
CXSL03zta+
soRTuwI/7J0
Q7gzwyJBuy
CYBn

ciphertext

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- Alice fetch happen. to make Stop trying Bob,

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)** :

ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**



- ο **Κρυπτογράφημα (ciphertext)**:

το τελικό μη αναγνώσιμο μήνυμα

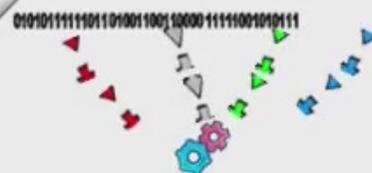
PIQ6NzOKW
CXSL03zta+
soRTuwI/7J0
Q7gzwyJBuy
CYBn

ciphertext

- ο **Κλειδί (key)**:

είναι μια **σειρά αρκετών bit**

που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.



Διαφορετικοί συνδιασμοί

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

- ο **Αποκρυπτογράφηση (Decryption)**:

η **αντίστροφη διαδικασία** της **κρυπτογράφησης**

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)**:

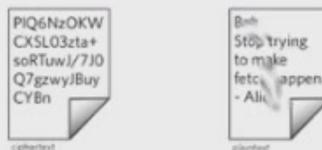
ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**

- ο **Κρυπτογράφημα (ciphertext)**:

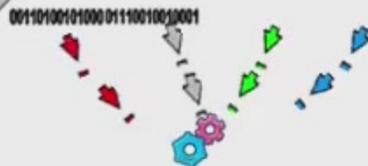
το **τελικό μη αναγνώσιμο μήνυμα**

- ο **Κλειδί (key)**:

είναι μια **σειρά αρκετών bit** που **χρησιμοποιείται ως είσοδος** στη **συνάρτηση κρυπτογράφησης**.



- Alice fetch happen. to make Stop trying Bob,



Διαφορετικοί συνδιασμοί

Κεφάλαιο 5ο

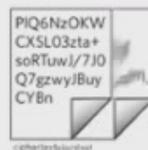
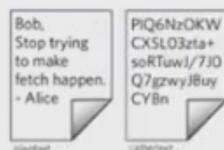
Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

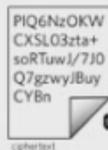
5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**
- ο **Απλό κείμενο (Plaintext)**:
το **αρχικό μήνυμα**
- ο **Αλγόριθμος κρυπτογράφησης (Cipher)** :
ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**
- ο **Κρυπτογράφημα (ciphertext)**:
το τελικό μη αναγνώσιμο μήνυμα
- ο **Κλειδί (key)**:
είναι μια **σειρά αρκετών bit** που **χρησιμοποιείται ως είσοδος** στη **συνάρτηση κρυπτογράφησης**.



Bob, fetch happen. to make Stop try PIQ6NzOKW



Διαφορετικοί συνδιασμοί

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

- ο **Αποκρυπτογράφηση (Decryption)**:

η **αντίστροφη διαδικασία** της **κρυπτογράφησης**

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)**:

ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**

- ο **Κρυπτογράφημα (ciphertext)**:

το **τελικό μη αναγνώσιμο μήνυμα**

- ο **Κλειδί (key)**:

είναι μια **σειρά αρκετών bit** που **χρησιμοποιείται ως είσοδος** στη **συνάρτηση κρυπτογράφησης**.

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext



CYBn Q7gzwyJBuy soRTuwJ/7J0 CXSL03zta+ PIQ6NzOKW

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext

00010001000001



Διαφορετικοί συνδιασμοί

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

- ο **Αποκρυπτογράφηση (Decryption)**:

η αντίστροφη διαδικασία της **κρυπτογράφησης**

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)**:

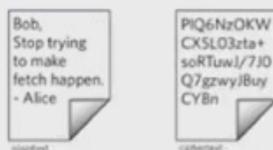
ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**

- ο **Κρυπτογράφημα (ciphertext)**:

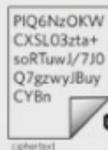
το τελικό μη αναγνώσιμο μήνυμα

- ο **Κλειδί (key)**:

είναι μια **σειρά αρκετών bit** που **χρησιμοποιείται ως είσοδος** στη **συνάρτηση κρυπτογράφησης**.



- Alice fetch happen. to make Stop trying Bob,



Διαφορετικοί συνδιασμοί

CAESAR CIPHER

https://www.youtube.com/watch?v=...

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

- ο **Αποκρυπτογράφηση (Decryption)**:

η **αντίστροφη διαδικασία** της **κρυπτογράφησης**

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)**:

ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**

- ο **Κρυπτογράφημα (ciphertext)**:

το **τελικό μη αναγνώσιμο μήνυμα**

- ο **Κλειδί (key)**:

είναι μια **σειρά αρκετών bit** που **χρησιμοποιείται ως είσοδος** στη **συνάρτηση κρυπτογράφησης**.

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

ciphertext

PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

ciphertext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- Alice fetch happen. to make Stop trying Bob,



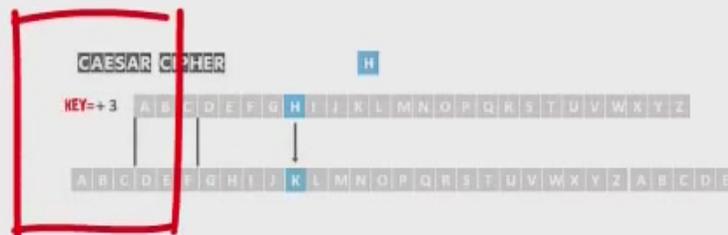
PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

ciphertext

00010001000001



Διαφορετικοί συνδυασμοί



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

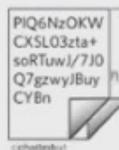
Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**
- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**
- ο **Απλό κείμενο (Plaintext)**:
το **αρχικό μήνυμα**
- ο **Αλγόριθμος κρυπτογράφησης (Cipher)**:
ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**
- ο **Κρυπτογράφημα (ciphertext)**:
το **τελικό μη αναγνώσιμο μήνυμα**
- ο **Κλειδί (key)**:
είναι μια **σειρά αρκετών bit** που **χρησιμοποιείται ως είσοδος** στη **συνάρτηση κρυπτογράφησης**.



Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext



PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

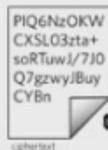
ciphertext



Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

Bob, fetch happen. to make Stop trying

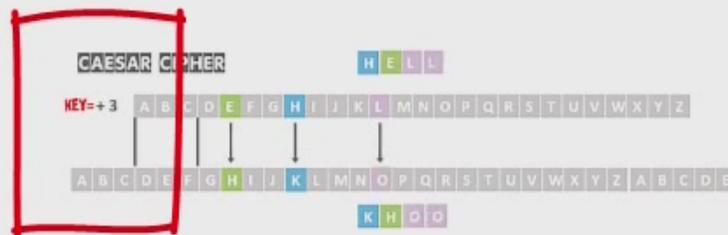


PIQ6NzOKW
CXSL03zta+
soRTuwI/7JO
Q7gzwyJBuy
CYBn

ciphertext

0011010010100001110010010001

Διαφορετικοί συνδιασμοί



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwI/7J0
Q7gzwyJBuy
CYBn

ciphertext

- ο **Αποκρυπτογράφηση (Decryption)**:

η **αντίστροφη διαδικασία** της **κρυπτογράφησης**

PIQ6NzOKW
CXSL03zta+
soRTuwI/7J0
Q7gzwyJBuy
CYBn

ciphertext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- Alice fetch happen. to make Stop trying Bob,

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)** :

ο **αλγόριθμος** (ο **τρόπος**) με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα** σε **μη αναγνώσιμο**



- ο **Κρυπτογράφημα (ciphertext)**:

το **τελικό μη αναγνώσιμο μήνυμα**

PIQ6NzOKW
CXSL03zta+
soRTuwI/7J0
Q7gzwyJBuy
CYBn

ciphertext

- ο **Κλειδί (key)**:

είναι μια **σειρά αρκετών bit** που **χρησιμοποιείται** ως **είσοδος** στη **συνάρτηση κρυπτογράφησης**.



Διαφορετικοί συνδιασμοί

CAESAR CIPHER

H E L L O

KEY=+3

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

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 A B C D E

K H O O R

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:

Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

- ο **Αποκρυπτογράφηση (Decryption)**:

η **αντίστροφη διαδικασία** της **κρυπτογράφησης**

- ο **Απλό κείμενο (Plaintext)**:

το **αρχικό μήνυμα**

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)**:

ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**

- ο **Κρυπτογράφημα (ciphertext)**:

το **τελικό μη αναγνώσιμο μήνυμα**

- ο **Κλειδί (key)**:

είναι μια **σειρά αρκετών bit** που **χρησιμοποιείται ως είσοδος** στη **συνάρτηση κρυπτογράφησης**.

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7JO
Q7gzwyJBuy
CYBn

ciphertext

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7JO
Q7gzwyJBuy
CYBn

ciphertext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

- Alice fetch happen. to make Stop trying Bob,



PIQ6NzOKW
CXSL03zta+
soRTuwJ/7JO
Q7gzwyJBuy
CYBn

ciphertext

0011010010100001110010010001



Διαφορετικοί συνδυασμοί

Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Χρήσιμη ορολογία στην **κρυπτογραφία** είναι η παρακάτω:

- ο **Κρυπτογράφηση (Encryption)**:
Η **διαδικασία μετασχηματισμού** του **μηνύματος** από το **αρχικό μήνυμα** στο **τελικό μη αναγνώσιμο**

- ο **Αποκρυπτογράφηση (Decryption)**:
η αντίστροφη διαδικασία της **κρυπτογράφησης**

- ο **Απλό κείμενο (Plaintext)**:
το **αρχικό μήνυμα**

- ο **Αλγόριθμος κρυπτογράφησης (Cipher)**:
ο **αλγόριθμος (ο τρόπος)** με τον οποίο θα **μετατραπεί** το **αρχικό μήνυμα σε μη αναγνώσιμο**

- ο **Κρυπτογράφημα (ciphertext)**:
το τελικό μη αναγνώσιμο μήνυμα

- ο **Κλειδί (key)**:
είναι μια **σειρά αρκετών bit** που **χρησιμοποιείται ως είσοδος** στη **συνάρτηση κρυπτογράφησης**.

Bob,
Stop trying
to make
fetch happen.
- Alice

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7JO
Q7gzwyJBuy
CYBn

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7JO
Q7gzwyJBuy
CYBn

Bob,
Stop trying
to n
fet
- Alice

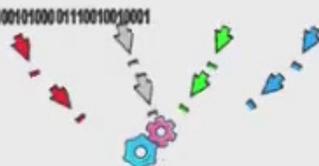
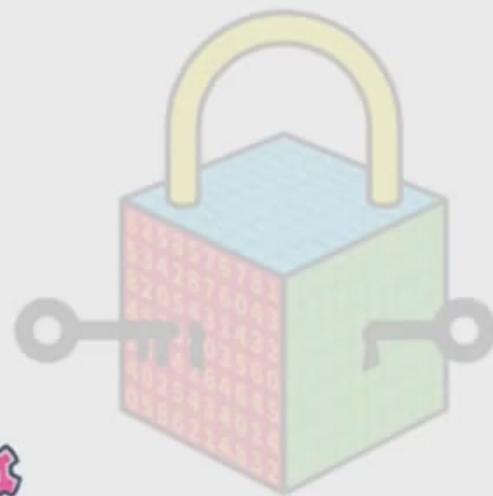
Bob,
Stop trying
to make
fetch happen.
- Alice

- Alice fetch happen. to make Stop trying Bob,

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7JO
Q7gzwyJBuy
CYBn

0011010010100001110010010001

Διαφορετικοί συνδιασμοί



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

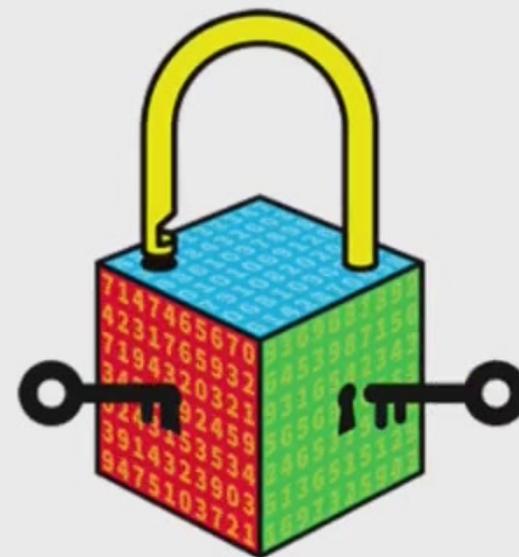
Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Στη μοντέρνα **κρυπτογραφία** υπάρχουν **δύο ειδών κρυπτογραφήσεις**.



Κεφάλαιο 5ο

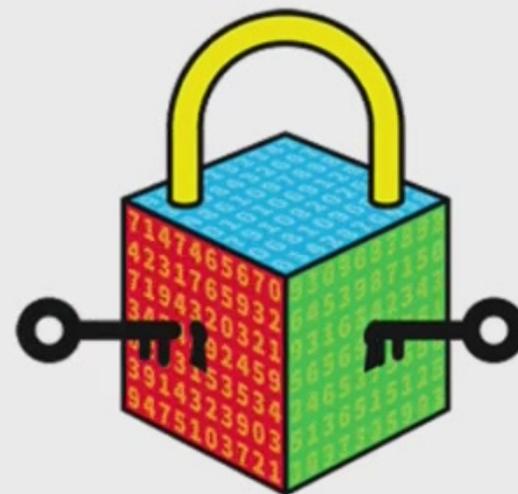
Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Στη μοντέρνα **κρυπτογραφία** υπάρχουν **δύο ειδών κρυπτογραφήσεις**,

Συμμετρικού κ



Κεφάλαιο 5ο

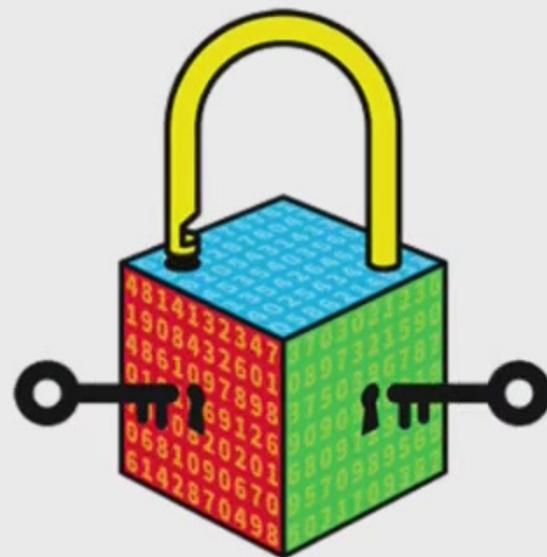
Ασφάλεια Πληροφοριακών Συστημάτων

5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Στη μοντέρνα **κρυπτογραφία** υπάρχουν **δύο ειδών κρυπτογραφήσεις**,

Συμμετρικού κλειδιού (Symmetric key) και



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

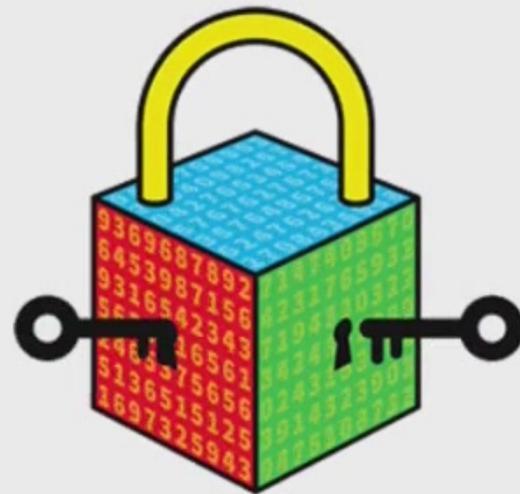
5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Στη μοντέρνα **κρυπτογραφία** υπάρχουν **δύο ειδών κρυπτογραφήσεις**,

Συμμετρικού κλειδιού (Symmetric key) και

Ασύμμετρου κλειδιού ή Δημοσίου κλειδιού (Asymmetric key - Public key).



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

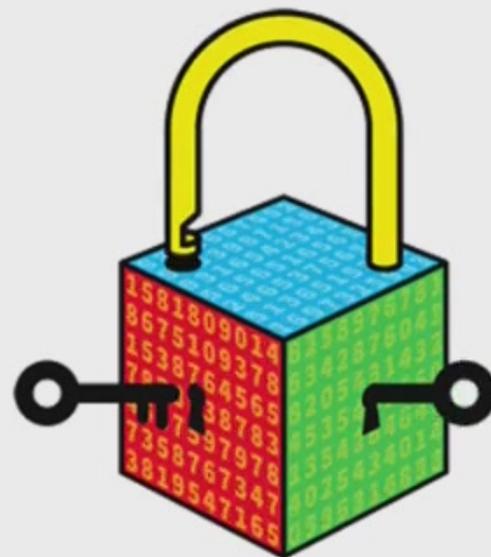
5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Στη μοντέρνα **κρυπτογραφία** υπάρχουν **δύο ειδών κρυπτογραφήσεις**,

Συμμετρικού κλειδιού (Symmetric key) και

Ασύμμετρου κλειδιού ή Δημοσίου κλειδιού (Asymmetric key - Public key).



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

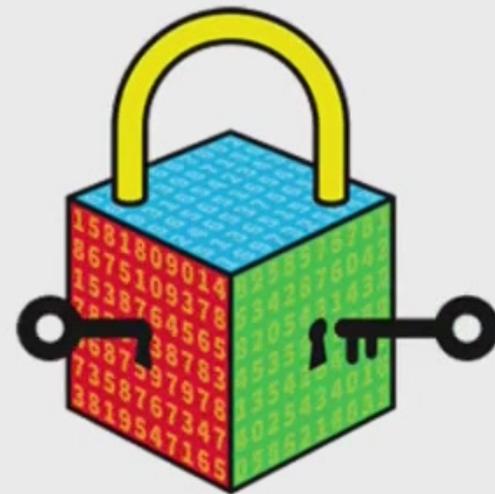
5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Στη μοντέρνα **κρυπτογραφία** υπάρχουν **δύο ειδών κρυπτογραφήσεις**,

Συμμετρικού κλειδιού (Symmetric key) και

Ασύμμετρου κλειδιού ή Δημοσίου κλειδιού (Asymmetric key - Public key).



Κεφάλαιο 5ο

Ασφάλεια Πληροφοριακών Συστημάτων

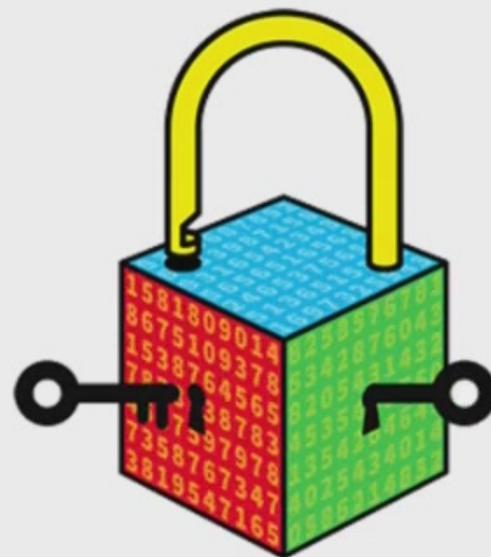
5.3 Ασφάλεια Λογισμικού

5.3.4 Κρυπτογραφία (Cryptography)

Στη μοντέρνα **κρυπτογραφία** υπάρχουν **δύο ειδών κρυπτογραφήσεις**,

Συμμετρικού κλειδιού (Symmetric key) και

Ασύμμετρου κλειδιού ή Δημοσίου κλειδιού (Asymmetric key - Public key).



ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



Spyros Zygouris
Informatics Professor

 spzygouris@gmail.com

You  Tube