Lecture 19 - Communications Security Principles

Exercise 1: How important are each of the above goals for the following applications: access to a news web site, downloading free software, web access to a banking system, deciding to allow access to an ISP's network.

app.	secrecy	auth. orig. / req dest.	integrity
news web site	N	N (Y?) / Y	Y
download free S/W	N	N / Y	Y
banking access	Y (most)	Y / Y	Y
access contrl	?	Y / ?	?

Exercise 2: Can you think of an example where metadata might need to be protected?

- criminal
- political
- financial

Steganography

↓

hiding the [encrypted] content "inside" other content

Exercise 3: If you could test one key per nanosecond, how long would it take, on average, to find the key if it was 32 bits long? 128 bits? 2048 bits?

$$2^{32} = 2\times2\times2^{30} = 4\times\left(10^{10}\right)^{3} = 4\times1000^{3} = 4\times10^{9}$$

4 seconds for 32 bit key.

$$2^{128} \approx \left(2^{10}\right)^{13} \approx \left(10^{3}\right)^{13} \approx 10^{39}$$

@ 1GHz = 10^{30} seconds.

$\approx 10^{22}$ years. $\simeq$ 4 million years

for a 128-bit key

seconds per 1year:

$3600 \approx 4000$

$\underline{\;20}$

8×10^{4} s/dy.

$\times$ 400 days/yr

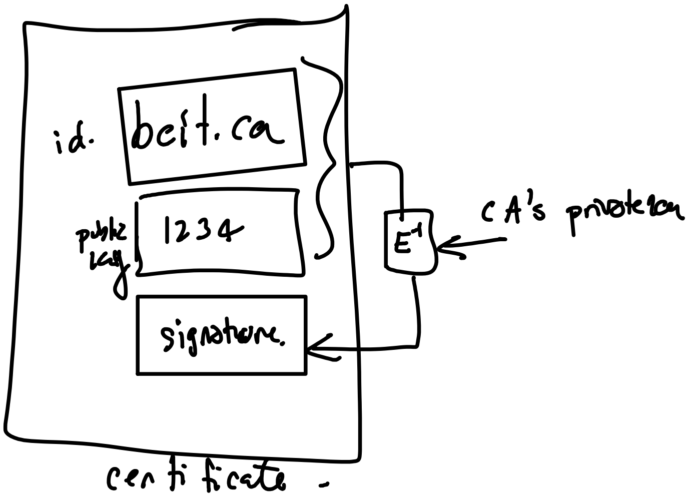
$= 32\times10^{6}$ s/year.

$\simeq 10^{8}$ s/yr

(actually 3×10^{7} s/year)

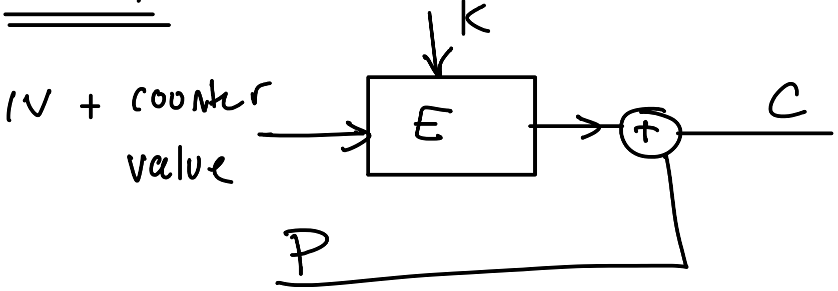
Exercise 4: Why does the signing key have to be kept private?

- otherwise anyone could sign the messages/digests.



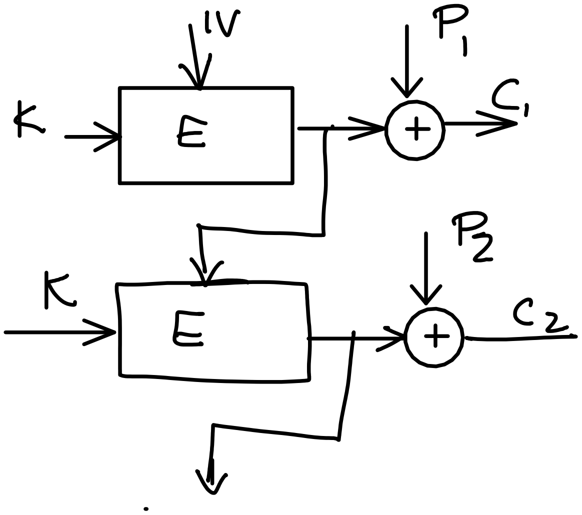
certificate -

CTR



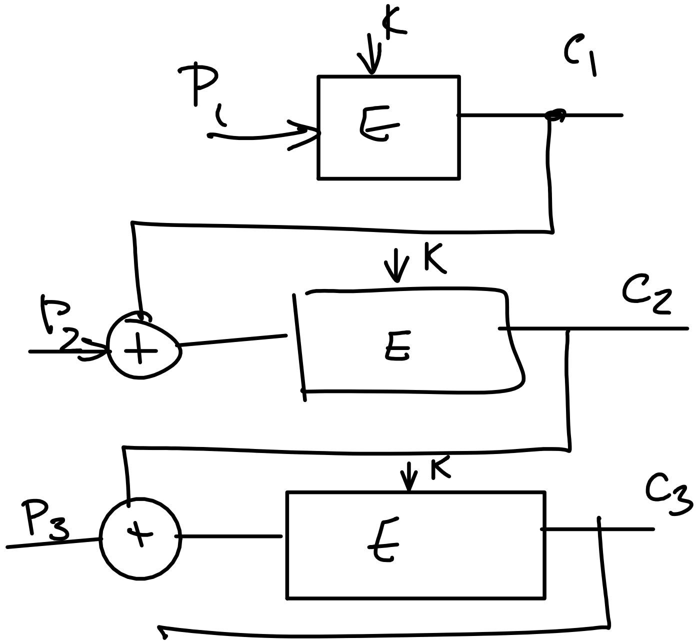
K
IV + counter value
E
+
C
P

OFB



IV
P_1
K
E
+
C_1
P_2
K
E
+
C_2

CBC



K
P_1
E
C_1
K
C_2
P_2
+
E
K
C_3
P_3
+
E