### page 1 (jeld)
hi im sadegh hayeri and want summary this IEEE article that name is DIGITAL RANDOMNESS

### page 2 (DIGITAL RANDOMNESS)
This article want to talk about Random numbers
and have two part
first talk about way random numbers are important
and then talk about how computers generate random numbers

### page 3 (Why random numbers are important?)
first
Why random numbers are important?
random is very very important in computers!
for example:

### page 4 (games)
games - most of games have random events!

### page 5 (visualization)
visualization - we need random numbers to make our visualization simalar to reality

### page 6 (security)
for security
every day you see websites like:

### page 7 (google)
google

### page 8 (digikala)
digikala

### page 9 (CAS)
central atenticate ?!!!!

### page 10 (saman)
bank payment pages and too many other websites

### page 11 (zoom saman)
and if you focus on url bar on top of your browser, you see the url goes to green color with green lock icon next to it!
its mean this web site use HTTPS connection,

### page 12 (http vs https)
two protocol used for webpages, one of is HTTP and other is HTTPS
when using HTTP, all of our requests and responds can be (شنود) by hackers with sample man in the middle attack,
but if using HTTPS, hackers cant see real content of requests because all requests encrypted!

### page 13 (HTTPS how works)
in https protocol client must generate an random and secure and Non-guessble string and send it to the server!

### page 14 (how generate random numbers in computers)
our computers go from deterministic woulds of zero and ons, and you can't write a code and run one time and get one output, and when run it again get other outputs
now how we can generate randomly numbers?

### page 15 (pseudorandom)
pseudorandom functions are function like this, these functions get an input number that name is seed, and generate pseudorandom numbers using that seed.
these numbers seems to be random but not really random,

### page 16 (check randomized)
for example if I get 100 to this function, that generate these numbers for me

### page 17 (other one)
and if other one get 100 to this function, he gets the same numbers of me!

these pseudorandom functions are very fast and can be use for example games, on visualities, but not good for security purposes!
and we need really random seeds to use these functions,
now how generate random seeds?!

### page 18 (lava lamps)
maybe you see these things in bedrooms
that name is lava lamps,
in 1997 they use these lamps to generate random numbers, they take a photo of these lamps and using images processing and bubble patterns, they generate random seeds!

### page 19 (thermal noise)
or they use thermal noises,
they get thermal noise with sensors, then amplifying it, then using special circuit to generate random numbers using that noise!

but these ways wasn’t really good!
because they:
use much more energy
they are very slow
its hard to maintain

### page 20 (Digital random generators)
Intel’s researchers make this circuit, the design includes a pair of inverters, they connect the output of one inverter to the other inverter’s input.
one of investors wants to make output to 1
and other one want to make it to 0
But which inverter should output which?

### page 21 (nemodarsh)
There are two possibilities
and the circuit can generate random 0 or 1 signals

if we want truly, this circuit isn’t really random too!
thermal noise, temperature, small difference in gates, can cause the circuit doesn’t work completely random, but if used for pseudorandom functions, the result is good for our purposes!

### page 22(tanks!)