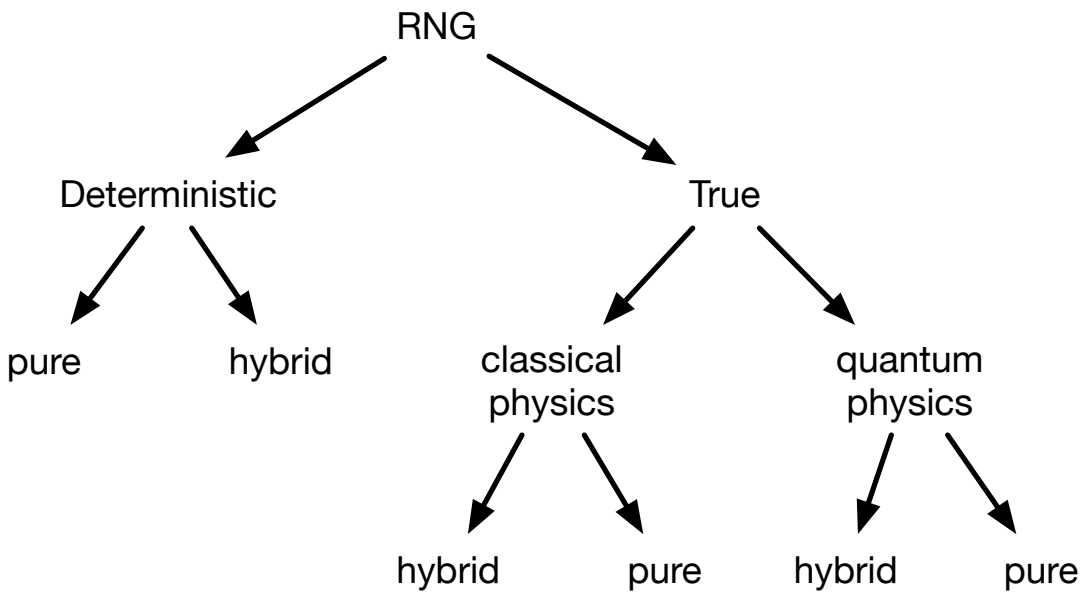
Random Number Generators



Random Numbers in Cryptography

- Session keys
- Signature keys and parameters
- Authentication protocols
- Ephemeral keys (DSA, ECDSA, ElGamal)
- Zero-knowledge protocols
- IVs for block ciphers
- Blinding and masking values

Properties of Random Numbers

Silent Requirement: The random numbers should assume **all admissible values with equal probability** and should be **independent from predecessors and successors**

This characterizes an ideal random number generator

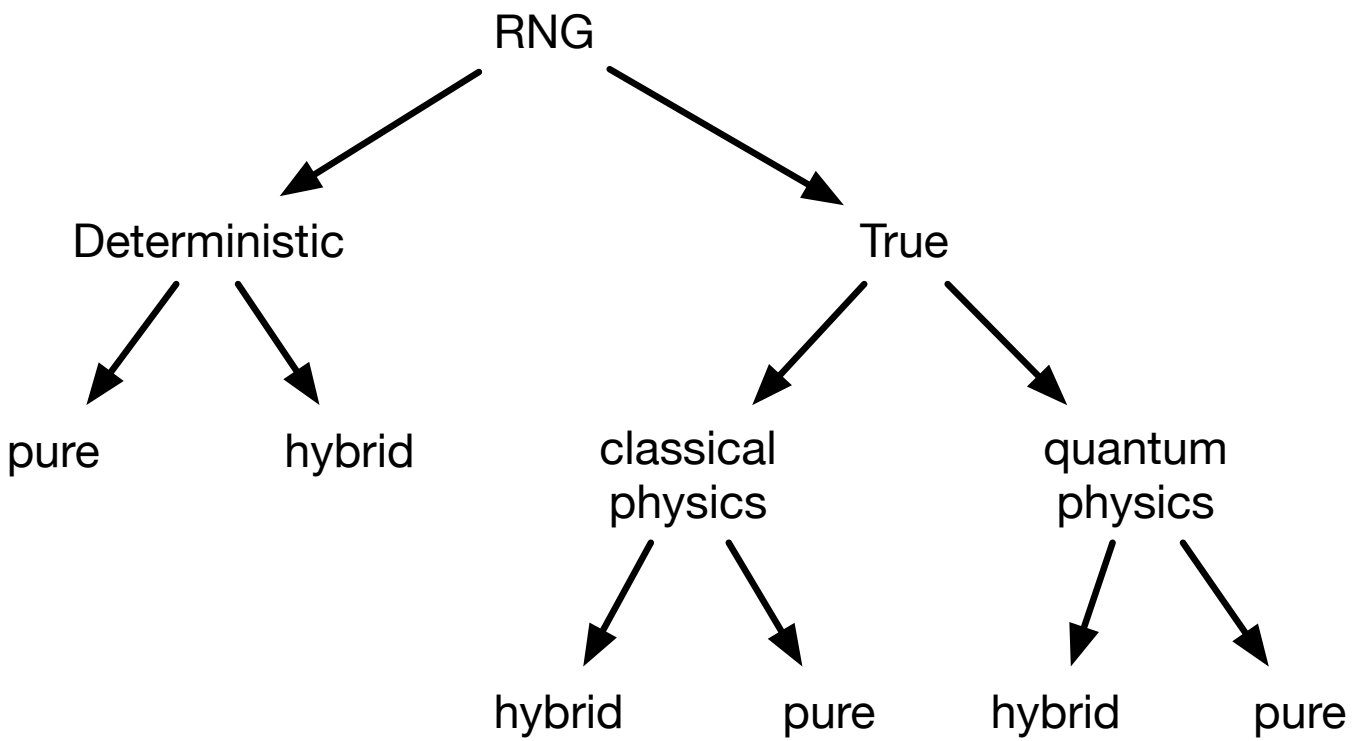
Ideal RNGs

- Even with maximal knowledge and unlimited computational power an attacker has no better strategy than "blind" guessing
  $\rightarrow$ Brute force attack

- Guessing n random bits costs 2^{n-1} trials in average
- The guess work should remain **invariant** in the course of time
  $\rightarrow$ Today
  $\rightarrow$ 2 years later
  $\rightarrow$ 100 years later

- However, An ideal RNG is a mathematical construct!

Real World RNGs



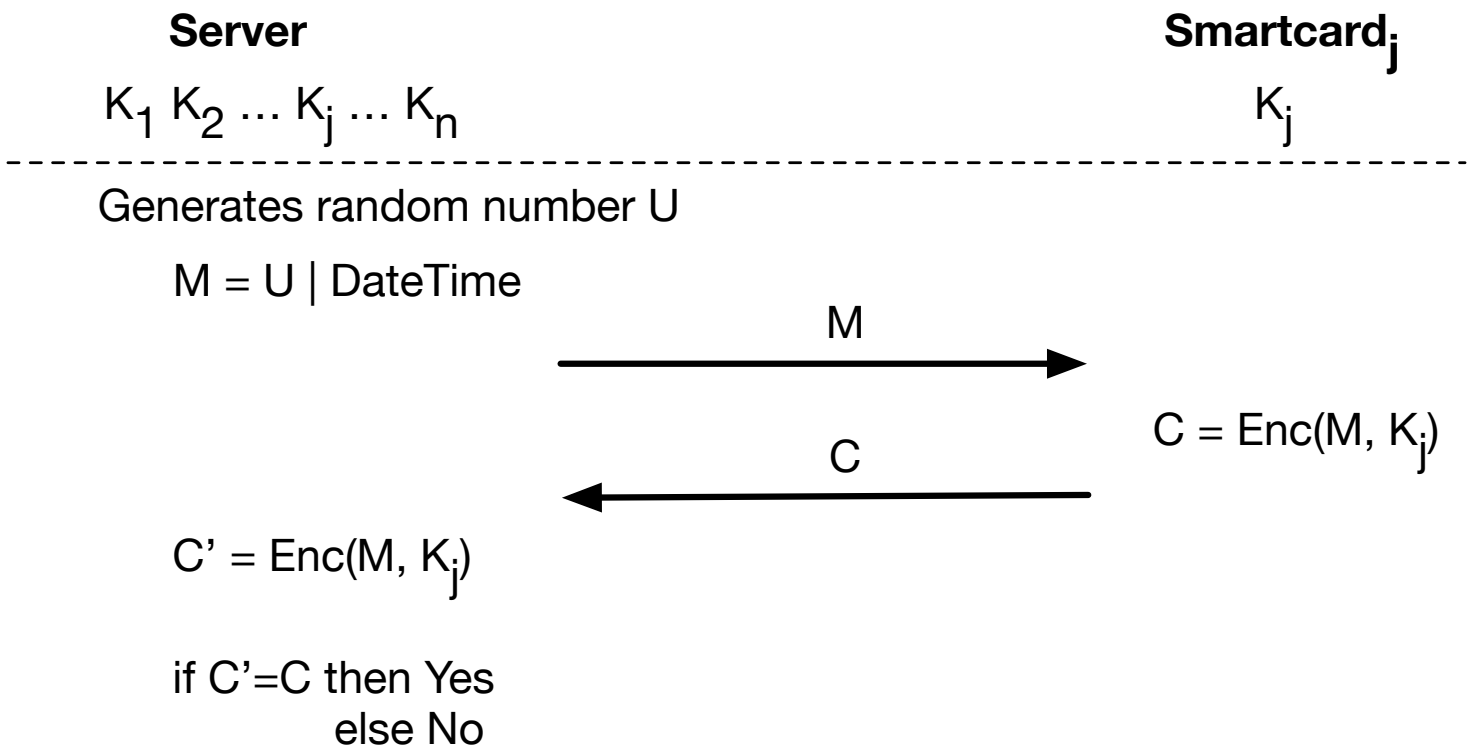
Deterministic RNGs in Cryptography

- Deterministic RNGs are also known as *pseudorandom* number generators (PRNGs)
- They are algorithmic and mathematical constructs
- Many algorithms exist: Block cipher and hash function based algorithms, Linear congruential generators, Linear and nonlinear feedback shift registers, Number-theoretic RNGs, and Elliptic curve RNGs

True RNGs in Cryptography

- True random numbers cannot be computed on deterministic computers
- They are best produced using physical RNGs which operate by measuring a specially prepared and controlled random physical process
- **Information-theoretic provable RNGs** seem to be possible only by exploiting randomness inherent to certain quantum systems

Challenge-Response Protocol



To prevent replay attacks the random numbers $U_1, U_2, \ldots$ should be distinct with overwhelming probability

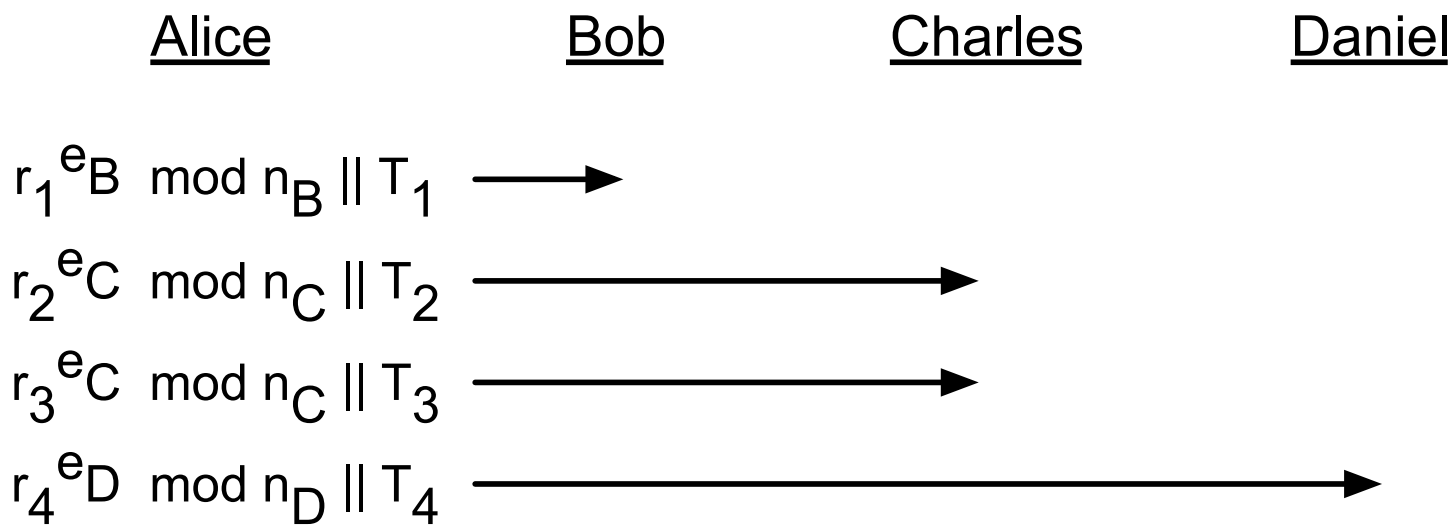
Security Requirement R1

- Random numbers should be **statistically independent** and **unbiased**

  - Probability of a number $\in \{1, 2, 3, 4, 5, 6\}$ does not depend on the previous number
  - Probability of a dice showing a number $\in \{1, 2, 3, 4, 5, 6\}$ is equal to $\frac{1}{6}$

- In other words, random numbers should not show any statistical weaknesses
- Requirement R1 is usually verified by statistical tests
- Is Requirement R1 is sufficient?

Key Exchange Protocol



Privileged attacker Charles:
The knowledge of r_2 and r_3 may allow him to guess r_1 or r_4

Security Requirement R2

- *The knowledge of subsequences of random numbers should not allow one to compute predecessors or successors practically or to guess them with non-negligibly larger probability than without knowledge of these subsequences*
- Requirement R2 means random numbers are unpredictable
- Requirement R2 implies backward and forward security
- Requirement R2 can be thought of as the union of
  R3: backward security and
  R4: forward security
  $R2 = R3 \cup R4$

Security Requirements

- The minimum requirements on the random numbers depend on the intended applications
- Requirement R2 is indispensable for generation of session keys or signature parameters
- Weakness or flaw in the RNG gives an attacker a significantly smaller search space
- The world of cryptography is full of spectacular failures

- RNG Failure $\Rightarrow$ Security Catastrophe

Netscape and SSL – 1996

DDJ, Jan96: Randomness and Netscape Browser https://www.cs.berkeley.edu/~daw/papers/ddj-netscape.html

Randomness and the Netscape Browser

January 1996 *Dr. Dobb's Journal*

How secure is the World Wide Web?

by Ian Goldberg and David Wagner

Our study revealed serious flaws in Netscape's implementation of SSL that make it relatively easy for an eavesdropper to decode the encrypted communications. Although Netscape has fixed these problems in a new version of their browser (as of this writing, Netscape 2.0 beta1 and Netscape Navigator 1.22 Security Update are available), these weaknesses provide several lessons for people interested in producing or purchasing secure software.

Netscape and SSL – 1996

The security of SSL, like that of any other cryptographic protocol, depends crucially on the unpredictability of this secret key. If an attacker can predict the key's value or even narrow down the number of keys that must be tried, the protocol can be broken with much less effort than if truly random keys had been used. Therefore, it is vital that the secret keys be generated from an unpredictable random-number source.

RNG Failure ⇒ Security Catastrophe

That was "old story"

Here are some new ones! :)

Real World Cryptography Conference
January 6-8, 2016

Brazilian Voting Machines

Software vulnerabilities in the Brazilian voting machine

Diego F. Aranha, UNICAMP
dfaranha@ic.unicamp.br
@dfaranha
http://www.ic.unicamp.br/~dfaranha

Brazilian Voting Machines

Brazilian DRE voting machines:
- **Claimed** 100% secure (but only tested in 2012...)
- Hardware manufactured by **Diebold** (> 0.5M)
- Software written by SEC since 2006 (> 13M LOCs)
- Adopted GNU/Linux in 2008 (after **Windows CE**...)
- Experimented with **paper records** in 2002
- Identify 16% of the voters with **fingerprints** since 2011

Brazilian Voting Machines

Brazilian Voting Machines

Inst. Federal de Educação Ciência
e Tecnologia do Rio Grande do Sul
Campus Bento Gonçalves

Zerésima

Eleição do IFRS
(28/06/2011)

Município 88888
Bento Gonçalves

Zona Eleitoral 0008
Seção Eleitoral 0021

Eleitores aptos 0083

Código identificação UE 01105161
Data 28/06/2011
Hora 08:32:08

RESUMO DA CORRESPONDÊNCIA
588.653

Brazilian Voting Machines

- Trivial to recover votes in order
- LOG associates vote with timestamp
- Thus trivial to recover a specific vote

Juniper's ScreenOS Backdoor

An update on the backdoor in Juniper's ScreenOS

Us: Stephen Checkoway, Shaanan Cohney, Matthew Green, Nadia Heninger, Eric Rescorla, and **Hovav Shacham**.
Important contributions by: H.D. Moore, Samuel Neves, Willem Pinckaers, and Ralf-Philipp Weinmann.

Juniper's ScreenOS Backdoor

Juniper security advisory, 17 Dec 2015

Administrative Access (CVE-2015-7755) allows unauthorized remote administrative access to the device. Exploitation of this vulnerability can lead to complete compromise of the affected device.

This issue only affects ScreenOS 6.3.0r17 through 6.3.0r20. **No other Juniper products or versions of ScreenOS are affected by this issue.**

Upon exploitation of this vulnerability, the log file would contain an entry that '**system**' had logged on followed by password authentication for a username.

Example:

Normal login by user **username1**:

```
2015-12-17 09:00:00 system warn 00515 Admin user username1 has logged on via SSH from …..
2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin
user 'username1' at host …
```

Compromised login by user **username2**:

```
2015-12-17 09:00:00 system warn 00515 Admin user system has logged on via SSH from …..
```

Juniper's ScreenOS Backdoor

ScreenOS was FIPS certified, but not with Dual EC

ScreenOS on NIST's RNG validation list: "ANSI X9.31 [TDES-3Key]".

But, from an October, 2013 Juniper Knowledge Base article:

The following product families do utilize Dual_EC_DRBG, but do not use the pre-defined points cited by NIST:

1. ScreenOS*

* ScreenOS does make use of the Dual_EC_DRBG standard, but is designed to not use Dual_EC_DRBG as its primary random number generator. ScreenOS uses it in a way that should not be vulnerable to the possible issue that has been brought to light. Instead of using the NIST recommended curve points it uses self-generated basis points and then takes the output as an input to FIPS/ANSI X.9.31 PRNG, which is the random number generator used in ScreenOS cryptographic operations.

From Russia with Hacks

Brendan I. Koerner. Russians Engineer a Brilliant Slot Machine Cheat And Casinos Have No Fix. *Wired*, February 6, 2017.

https://www.wired.com/2017/02/russians-engineer-brilliant-slot-machine-cheat-casinos-no-fix

From Russia with Hack

Breaking the System

2009 - Russia Outlaws all gambling.

Machines sold cheaply to shady people.

Modus Operandi

- Record ~ 24 games
- Upload recording to St. Petersberg
- Receive timing markers. (0.25s delay)
- With each vibration, hit spin!
- $$$

Are you feeling lucky?

From Russia with Hack

Let's talk numbers

25 Alleged Operatives

$1,000 oer machine

$10,000 per operative per day

$250,000 per 4-Person team per week

Casinos stiked in California, St. Louise, New Orleans, Missouri, Macao, Romania, Singapore, Peru

4 Operatives caught - syndicate runs rampant.

Artistocrat, Novomatic → "Machines are cracked, get rid of them"

New Machines use "PRNGs that use encryption to protect mathematical secrets"