Exam 2

TRAFO. ST. 10
Høyspenning
Livsfare

A backdoored PRNG

s_k — Internal PRNG states

r_k — Outputs

$f(\bullet)$ — State update function

$g(\bullet)$ — Output function

$h(\bullet)$ — Backdoor function

🟥 — Attacker computation

$$\begin{tikzcd}
s_0 \arrow[r, "f(s_0)"] \arrow[d, "g(s_0)"'] & s_1 \arrow[r, "f(s_1)"] \arrow[d, "g(s_1)"'] & s_2 \arrow[r, "f(s_2)"] \arrow[d, "g(s_2)"'] & s_3 & \\
r_1 & r_2 \arrow[ur, "h(r_2)"] & r_3 & & \cdots
\end{tikzcd}$$

ScreenOS 6.2 PRNG

```
char output[32];    // PRNG output buffer
int  index;         // Index into output
char seed[8];       // X9.31 seed
char key[24];       // X9.31 key
char block[8];      // X9.31 output block
int  reseed_counter;

void x9_31_reseed(void)
  reseed_counter = 0;
  if (dualec_generate(output, 32) != 32)
    error("[...]PRNG failure[...]", 11);
  memcpy(seed, output, 8);
  index = 8;
  memcpy(key, &output[index], 24);
  index = 32;
}
```

32 bytes from Dual EC stored in output

index set to 32

```
void prng_generate(voi
  int time[2] = { 0, g
  index = 0;
  ++reseed_counter;
  if (!one_stage_rng(
    x9_31_reseed();
  for (; index < 32; index += 8) {
    // FIPS checks removed for clarity
    x9_31_gen(time, seed, key, block);
    // FIPS checks removed for clarity
    memcpy(&output[index], block, 8);
  }
}
```

index set to 0

Always returns false*; reseed on every call

Loop never executes!

output still contains 32 bytes from Dual EC

* Can be disabled

Desirable properties of voting systems

Voter feels that:

- Vote was counted
- Vote was private
- Nobody else can vote more than once
- Nobody can alter others’ votes

People believe that the machine works correctly and that its behavior cannot be modified

These have to do with perception.

It is also important that these perceptions are true.

“The purpose of an election is to convince the supporters of the losing candidate that they lost”

J. Alex Halderman, University of Michigan

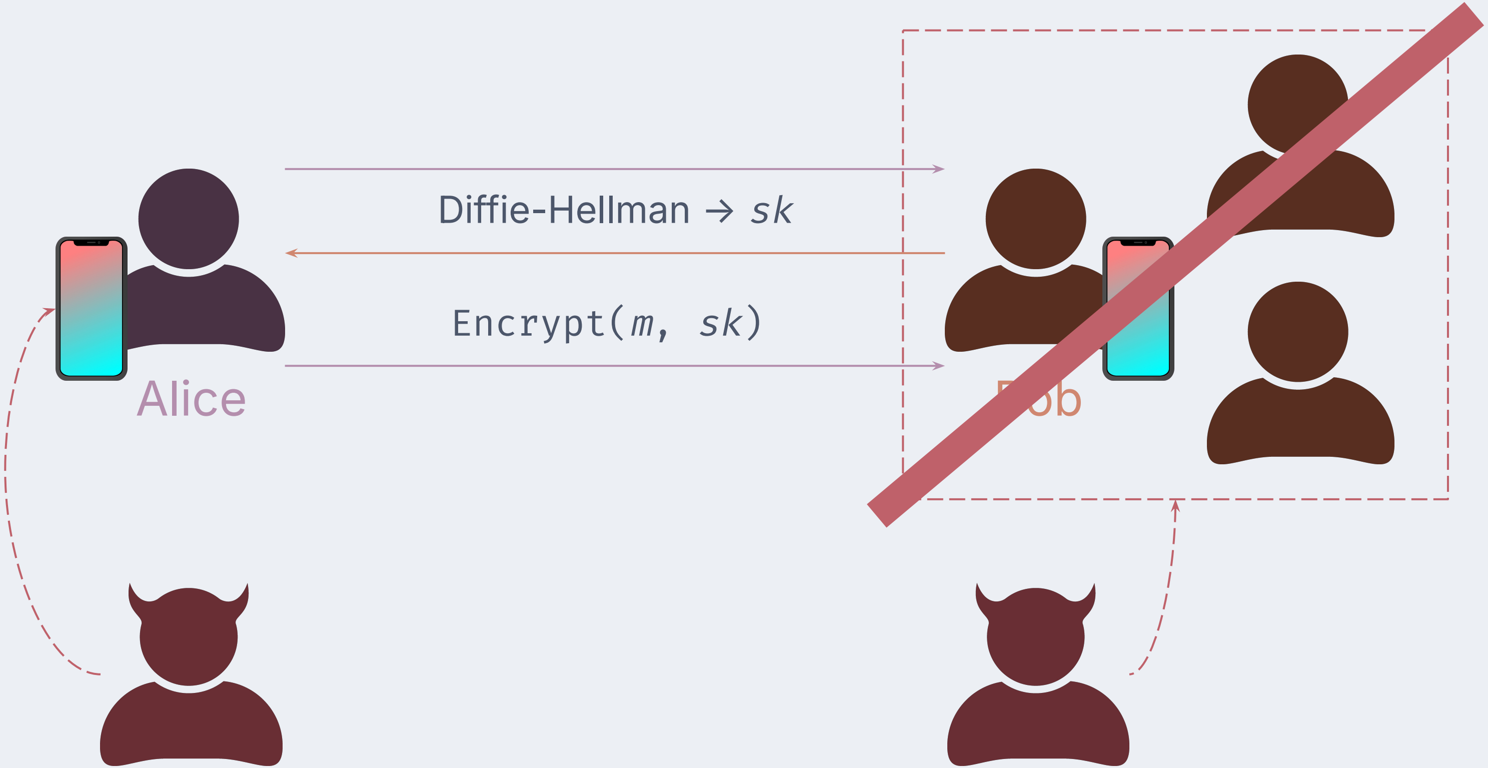
```
// LCG - Linear Conguential Generator
// used to generate ballot serial numbers
// A psuedo-random-sequence generator
// (per Applied Cryptography,
// by Bruce Schneier, Wiley, 1996)
```

`BallotResults.cpp`

Diebold Election Systems

“Unfortunately, linear congruential generators **cannot be used for cryptography**”

Bruce Scheiner
Applied Cryptography (Wiley, 1996)
Page 369



Diffie-Hellman → sk

`Encrypt(`m`, `sk`)`

Alice

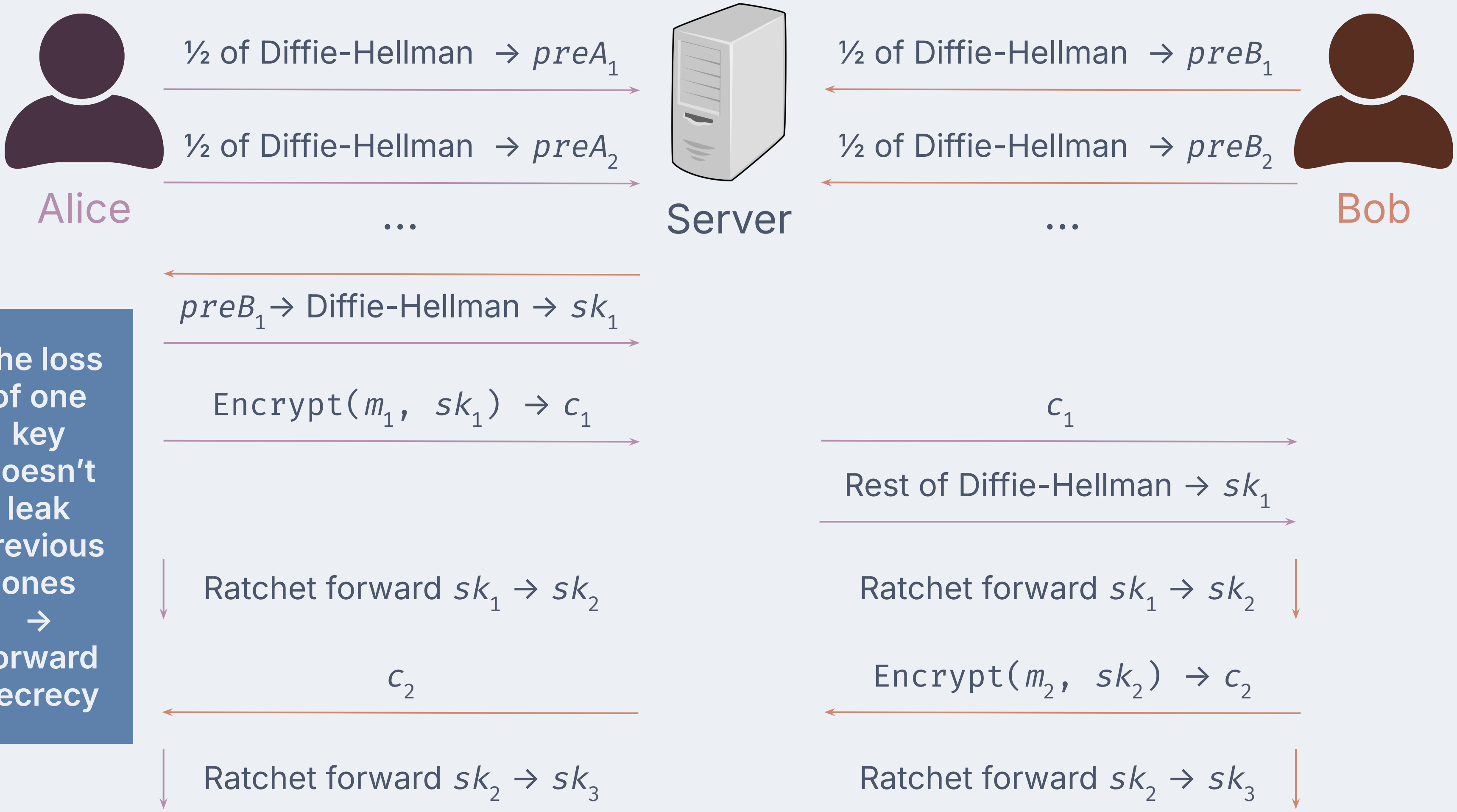
Bob

The importance of secure messaging

- Facebook Messenger, Instagram are not “end-to-end”
  - Facebook reads the messages, delivers ads about them
  - Governments can subpoena Facebook for your messages, reconstruct your digital life
- “Surveillance capitalism”
  - The person is the product
  - “Free” services provided by Big Tech powered by the selling of your data
- Data sharing agreements
  - Seen ads for things you’ve talked about on Amazon?

“But I have nothing to hide!”

- Solidarity with those who do
  - Snowden/whistleblowers, but also “The Feeling of Being Watched” subjects
- You might not realize how much data is out there
  - “We kill people based on metadata”
- Data lasts forever, and you might have to someday
  - Data lasts *forever* -- and companies/banks/governments are looking



Alice

Server

Bob

½ of Diffie-Hellman → $preA_1$

½ of Diffie-Hellman → $preA_2$

…

½ of Diffie-Hellman → $preB_1$

½ of Diffie-Hellman → $preB_2$

…

$preB_1$ → Diffie-Hellman → sk_1

$\texttt{Encrypt}(m_1,\ sk_1) \to c_1$

c_1

Rest of Diffie-Hellman → sk_1

Ratchet forward $sk_1 \to sk_2$

Ratchet forward $sk_1 \to sk_2$

c_2

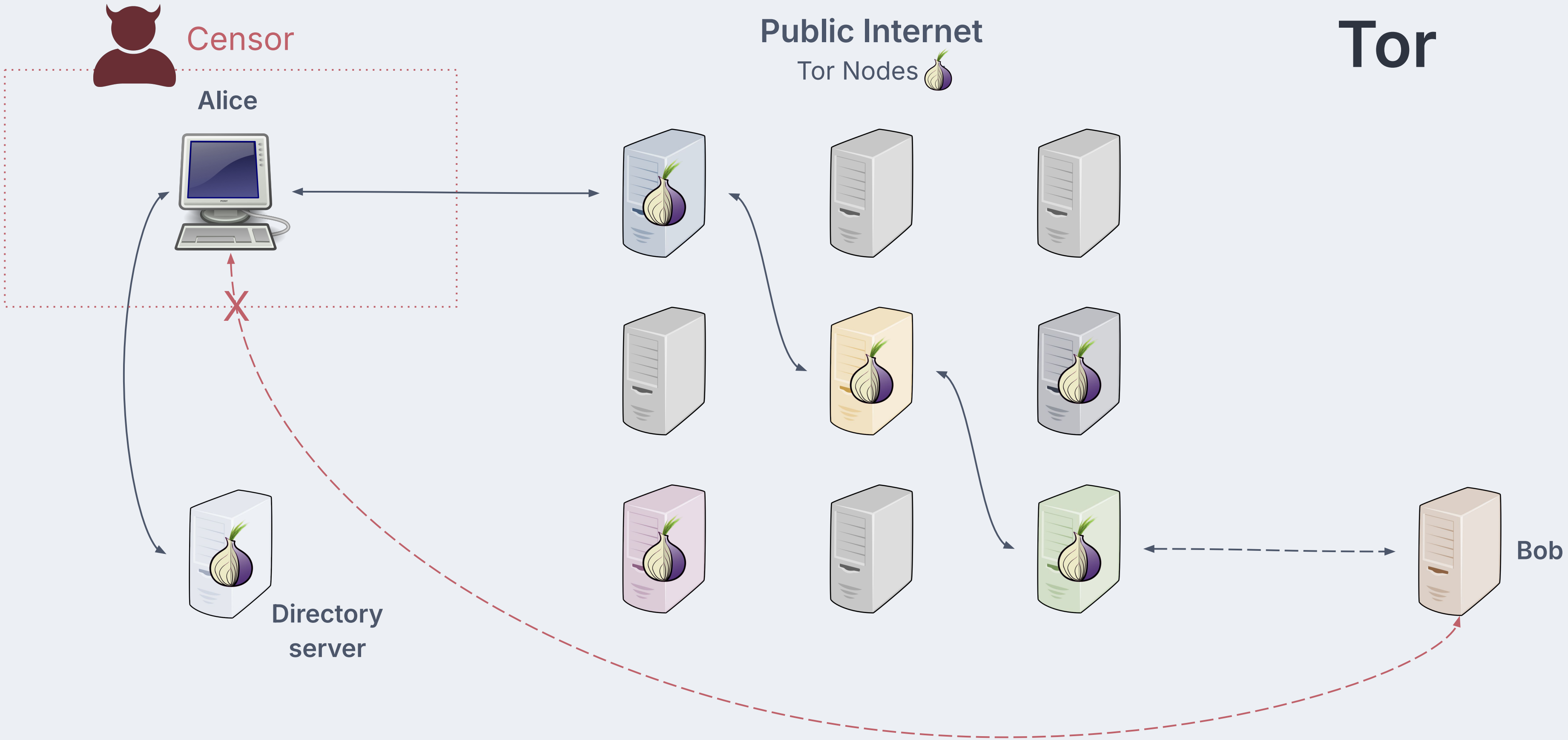
$\texttt{Encrypt}(m_2,\ sk_2) \to c_2$

Ratchet forward $sk_2 \to sk_3$

Ratchet forward $sk_2 \to sk_3$

The loss of one key doesn't leak previous ones → forward secrecy

Tor



Censor

Alice

Public Internet

Tor Nodes

Directory server

Bob

Threat Model

- Patient harm and non-harm risks
  - Pump delivers too much, not enough insulin
  - Pump leaks logs to unauthorized users

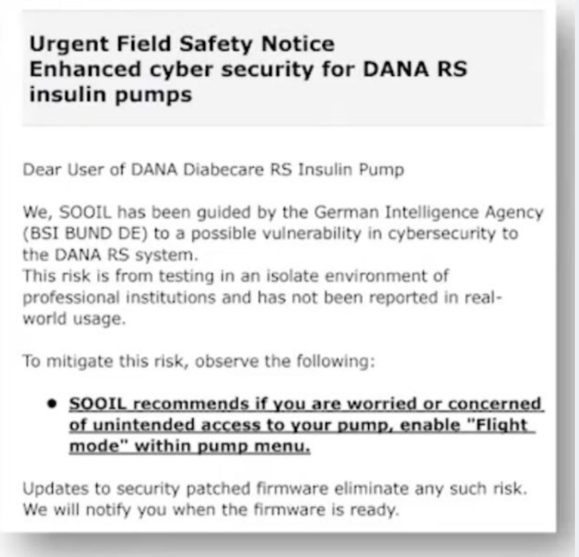
- Microsoft STRIDE
  - **S**poofing: Impersonate system
    - Attacker masquerades as smartphone

  - **T**ampering: Modify data or code
    - Attacker MITMs pump-to-smartphone communication

  - **R**epudiation: Claiming to not have performed an action
    - Pump audit log cannot distinguish unauthorized commands

Remediation, Temporary Measures & Disclosure

- Remediations are Complex:
  - Most vulnerabilities are design defects
  - The manufacturer prepared and rolled out a firmware update for the insulin pump in 04/2020.
- Operations is key:
  - Disable the insulin pump’s BLE functionality → airplane mode→ Preserve the pump‘s therapeutic purpose
  - The device implements safety features
- Disclosure managed by the ManiMed project team
  - A publication of the vulnerabilities does not pose serious risks or harm to patients as short-term measures or workarounds exist that preserve the pump‘s therapeutic purpose



Urgent Field Safety Notice
Enhanced cyber security for DANA RS insulin pumps

Dear User of DANA Diabecare RS Insulin Pump

We, SOOIL has been guided by the German Intelligence Agency (BSI BUND DE) to a possible vulnerability in cybersecurity to the DANA RS system.
This risk is from testing in an isolate environment of professional institutions and has not been reported in real-world usage.

To mitigate this risk, observe the following:

- **SOOIL recommends if you are worried or concerned of unintended access to your pump, enable "Flight mode" within pump menu.**

Updates to security patched firmware eliminate any such risk. We will notify you when the firmware is ready.

[https://advancedtherapeutics.org.uk/wp-content/uploads/2020/03/User-FSN-DANA-RS-Cybersecurity-002-6-March-2020.pdf, accessed July 28,2020]

DIY Diabetics Community

- Julian, Dina’s disclosure stirred up mixed feelings from the community
  - DANA RS remediations broke AndroidAPS compatibility

- Public service announcement:
  - We support the DIY Diabetics community, their hard work, and dedication
    - 11,896+ people using DIY Closed-loop systems as of May 11th, 2020[1]
    - 24,000,000+ loop hours[1]

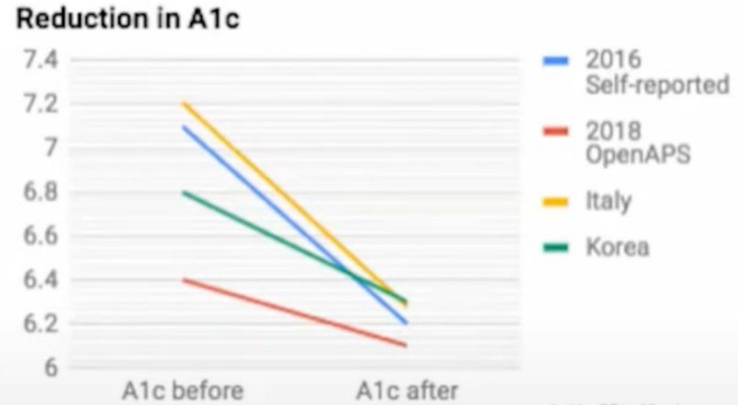


chart by @DanaMLewis

[1] https://openaps.org/outcomes/