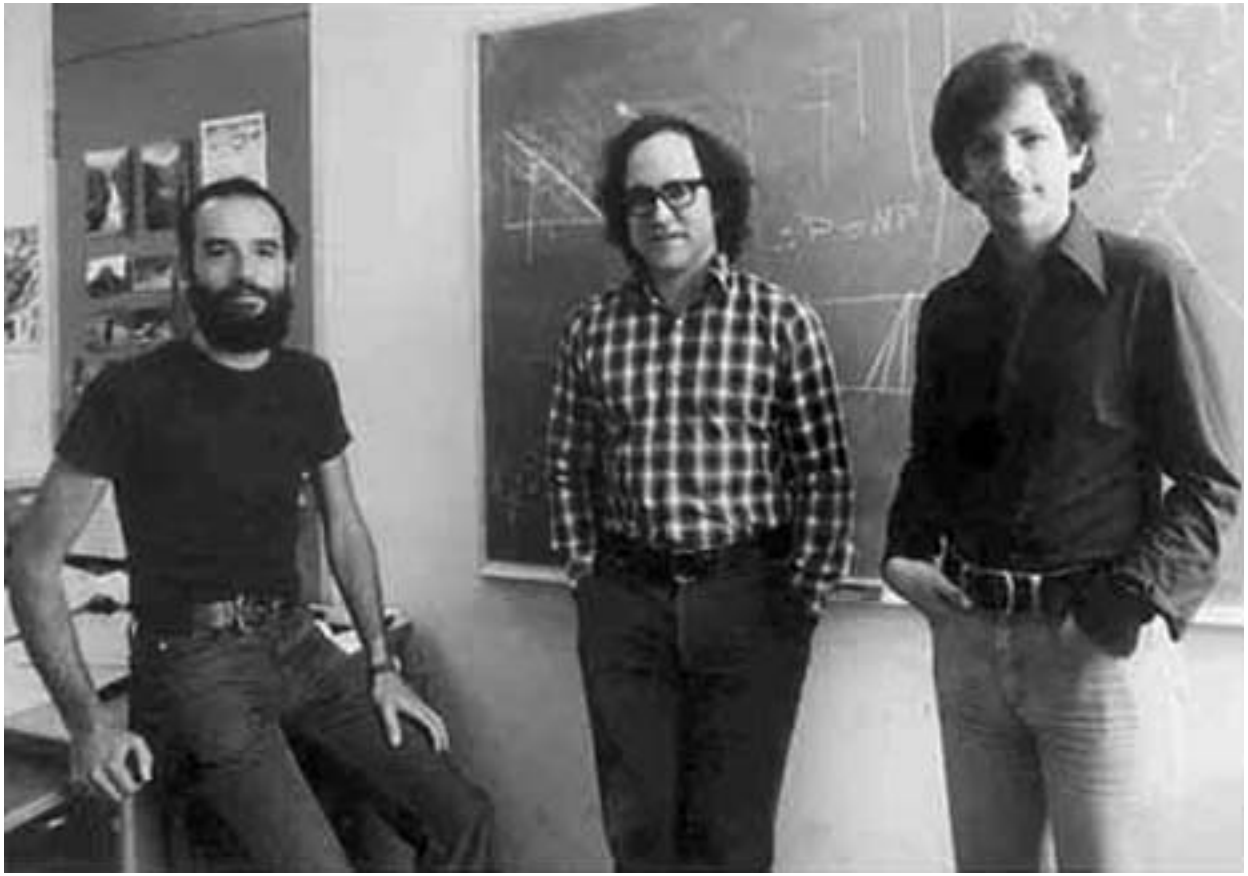
RSA: From Theory to Practice

CS5431

February 17, 2017

RSA



Finite Math

0,1, 2, 3, 4, 5, 6, 7, 8, 9,10, …

$$1 + 4 = 0$$
$$2 + 4 = 1$$
$$3 * 4 = 2$$
$$4 * 4 = 1$$

RSA

- Pick primes p, q
- Choose e, d such that $ed = 1 \bmod (p-1)(q-1)$
- $PK = (n, e)$
- $SK = (p, q, d)$

$$c = m^e \bmod n$$

$$m = c^d \bmod n$$

Chinese Remainder Algorithm

- Pick primes p, q
- Choose e, d such that $ed = 1 \bmod (p-1)(q-1)$
- $PK = (n, e)$
- $SK = (p, q, q^{-1} \bmod p, d, d \bmod p - 1, d \bmod q - 1,)$

$$c = m^e \bmod n$$

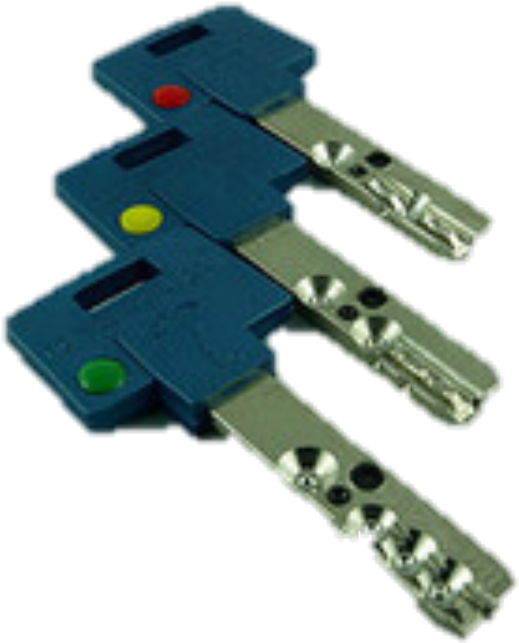
$$m_1 = c^{d \bmod p-1} \bmod p,$$
$$m_2 = c^{d \bmod q-1} \bmod q,$$
$$h = q^{-1}(m_1 - m_2) \bmod p,$$
$$m = m_2 + hq$$

Square-and-Multiply

```
res = 1;
while (exp > 0) {
        if (exp % 2 == 1){
                res = res * base % p;
        }
        base = base^2 % p;
        exp >> 1;
}
return res;
```

Beyond Theory…

Choosing Good Keys

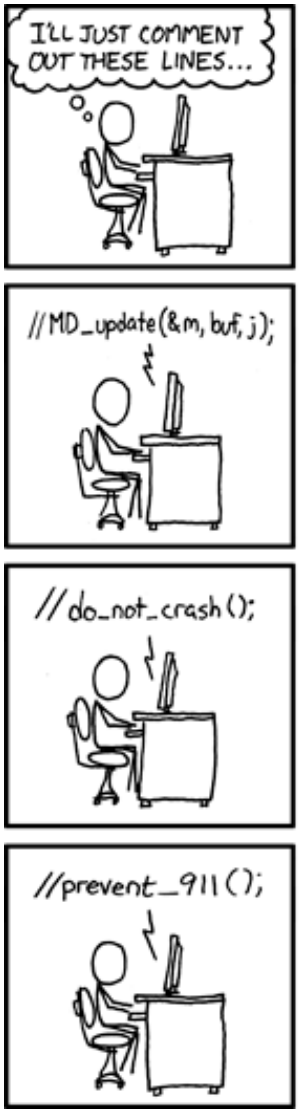


Randomness Quality

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Netscape

Debian Randomness

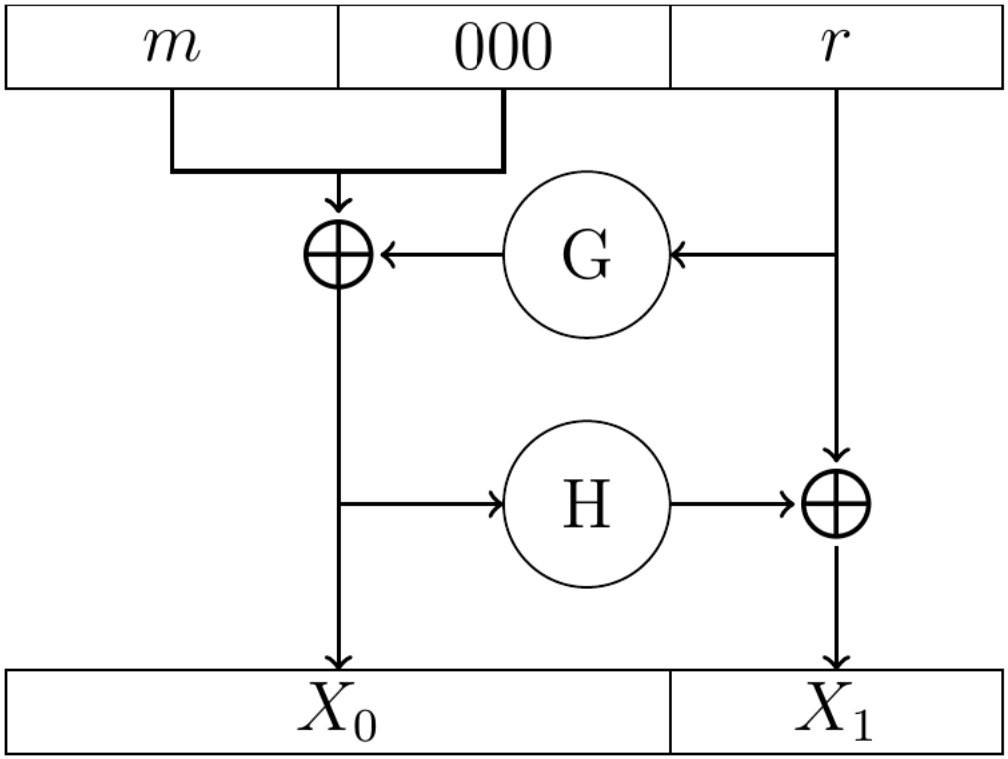


IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:

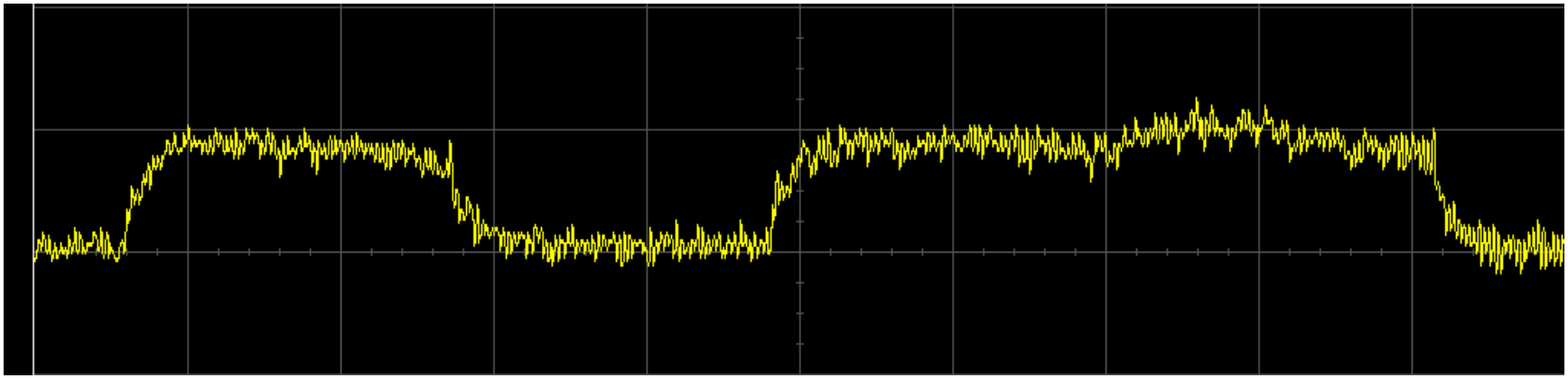
AFFECTED SYSTEM	SECURITY PROBLEM
FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
XANDROS (EEE PC)	GIVES ROOT ACCESS IF ASKED IN STERN VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ELVISH WORD FOR "FRIEND"
UBUNTU	TURNS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES

The Internet of Keys

Padding



Side Channels



- Power
- Timing
- EM Radiation
- Acoustics

Blinding