Open encryption technology - a contribution to a meso-level analysis of 'technical' factors

1st Nordic STS Conference
24.-26. april 2013
Trondheim, Norway

Niels Jørgensen
Roskilde University, Denmark

Research questions

How did present day, open encryption evolve?

- 2000+: encryption is a fully open technology
- 1970-80s: semi-open
- (before ~1970: secret, used by military and diplomacy)

Specific questions:

how did US government

- *.. succeed in preventing strong encryption in the 1970s*
- *.. but fail to do the same in the 1990s?*
- *What was the role of technical factors?*

Previous studies

Accounts by participants in the 1990s' debates:

Economics

- Businesses required strong encryption
- Diffie & Landau: “Privacy on the line” (2007)

Politics, activism

- “Privacy advocates convinced the government..”
- NSA Director McConnell (The New Yorker, 2008)

Technical

- The government's compromise (the Key Escrow Standard) was technically flawed, *probably technically infeasible*
- Matt Blaze: “Encrypting history at the NSA” (2008)

Research approach

Inspiration:

Schmidt & Werle (1998)
- standards in telecommunication
- constructivist, institutional, actor-centered

Misa (2009)
- meso-level analysis

Also
- it is meaningful to speak of technical factors, social factors,..
- a “mildly” constructivist approach ? (Bijker 2010)

Plan of talk

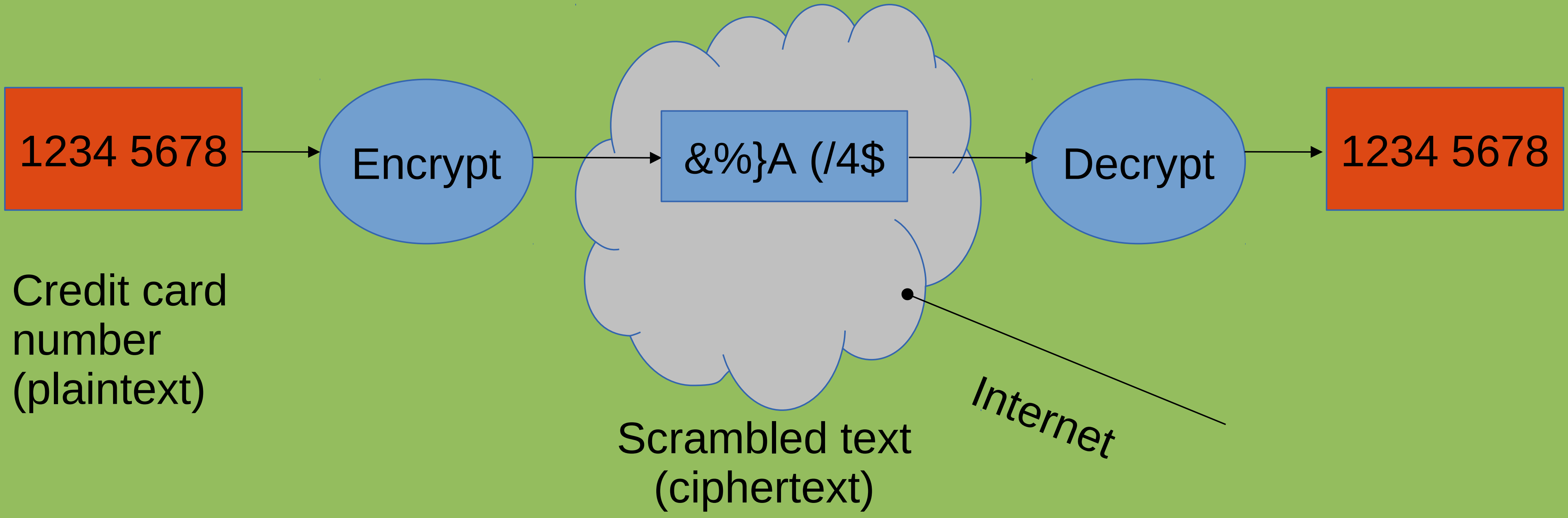
1. Background

- overview of development 1970-2000
- explain encryption
- and closed vs. open encryption

2. Analysis

- technical factors

Encryption



Encryption

- to make a text unreadable
- by “scrambling”
- yet the legitimate receiver can re-create the text

Today: strong & open encryption

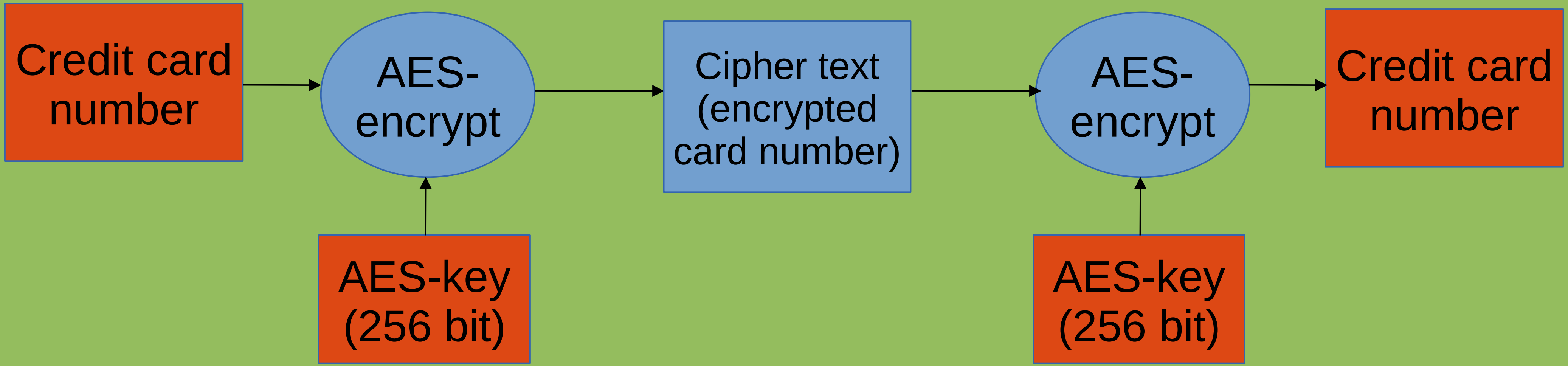
AES is the most widely used encryption algorithm by PC web browsers

- Firefox, Safari, Chrome, Explorer (newer)

AES:

- Advanced Encryption Standard
- Defined in 2001
- strong
- open
- aka. Rijndael (~ Rijmen + Daemen)

AES is “strong” encryption



Strong
•suppose attacker has ciphertext + algorithm
•can decrypt only using brute force (all keys = 2^{xx} or 2^{256})

“Unbreakable in practice”
•no proof that method is unbreakable
•so far nobody knows how to break the AES algorithm
•a pragmatic notion of strength (social, trust-based)

AES is “open” encryption

AES's definition is publicly available (and freely)
- FIPS Standard #197 (in 2001)
- explained on Wikipedia and at universities

AES implementations are publicly available (and freely)
- in web browsers
- open source libraries, eg. www.bouncycastle.org (java, C#)
- implementations can achieve certification

AES's design is discussed publicly
- by experts in academia and industry
- weaknesses ~ what are the best attacks on AES?
- strengths ~ the underlying math structure (a Galois field)

Legal to use in nearly all Western countries
Legal to export (with some restrictions)

1970s, 80s:
semi-open, semi-strong encryption

ATMs introduced in Denmark in 1984

- for users with Dankort credit cards

Encryption needed to protect data sent between the ATM and the bank

Only one realistic algorithm: DES

- Digital Encryption Standard
- a compromise
  - business interest: data protection
  - National Security Agency (NSA): prevent bad guy's access to strong encryption

DES is only semi-strong

Defined in 1977 by Federal Bureau of Standards

The bureau allowed changes by NSA

NSA reduced to key length fra 64 to 56 bits

- brute force attack needs to consider 2^{56} keys
- instead of 2^{64} keys

DES is only semi-open

DES was publicly available (and freely)

- FIPS #46

But the “design rationale” was secret

- NSA changed the “scrambling” function
- that is, the heart of the algorithm, the S-boxes
- NSA refused to say why

Suspicion

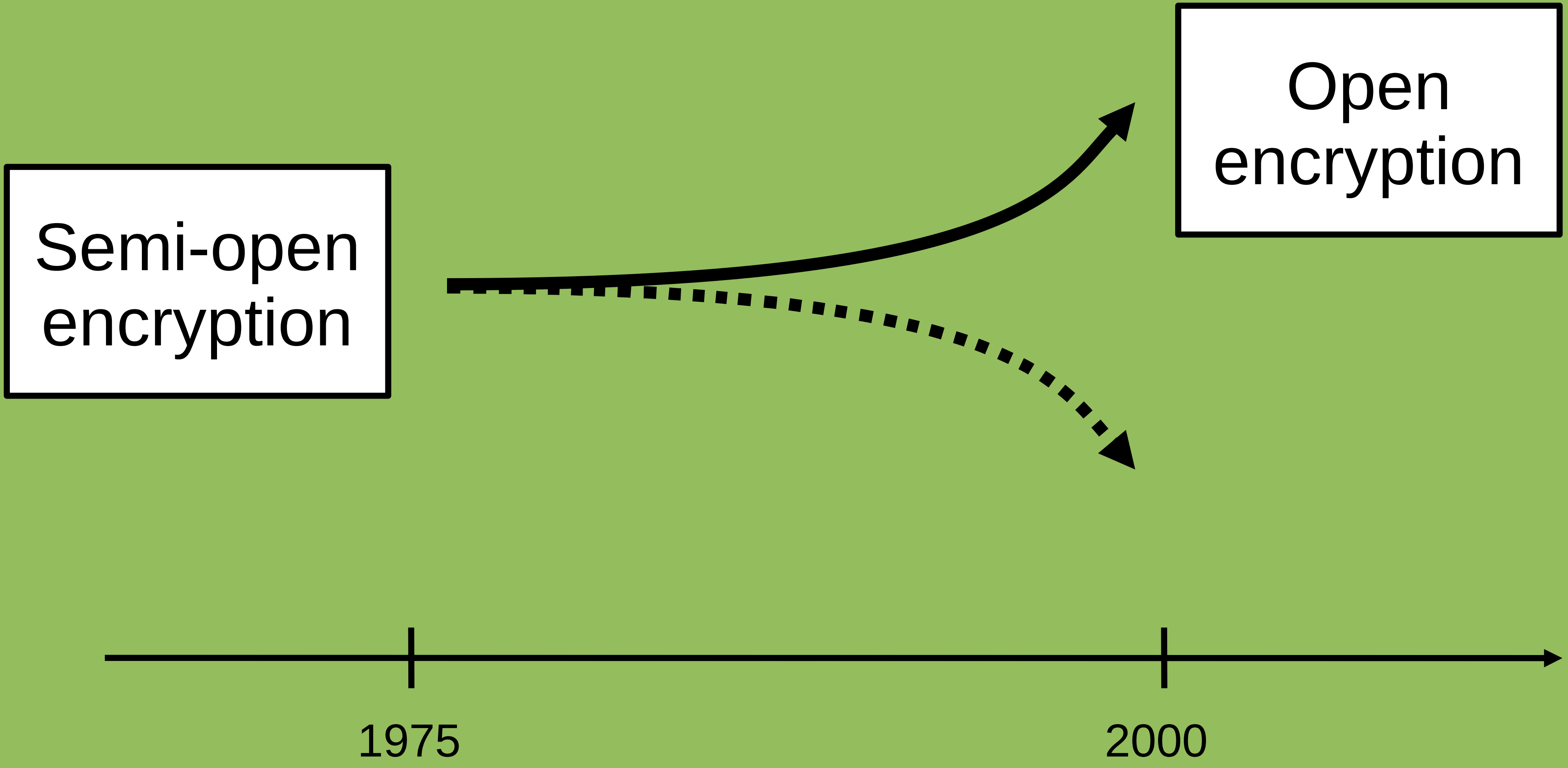
- had NSA inserted a “backdoor”?
- so that NSA could decrypt any message?

Plan of talk

1. Background
- overview of development 1970-2000
- explain encryption
- and closed vs. open encryption

2. Analysis
- technical factors

From semi-open to open encryption - the role of technical factors?



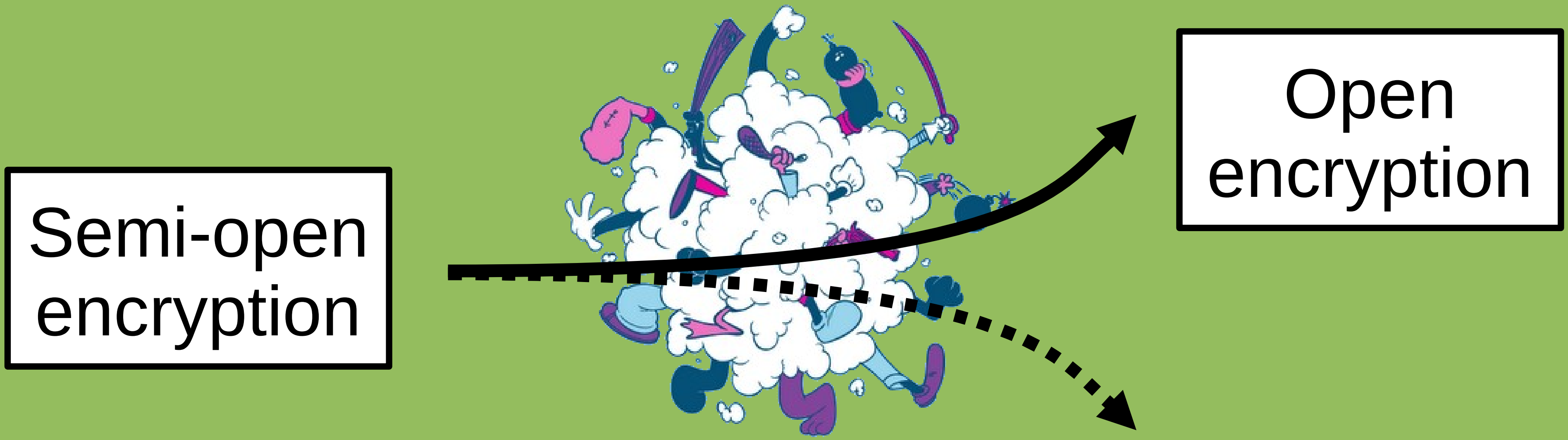
Semi-open encryption

Open encryption

1975

2000

Non-technical factors:
Social groups (cf. SCOT)



Semi-open encryption

Open encryption

Law enforcement:

- *“encryption threatens public safety”, “used by criminals”*

Business:

- *“encryption is needed to protect business secrets”*

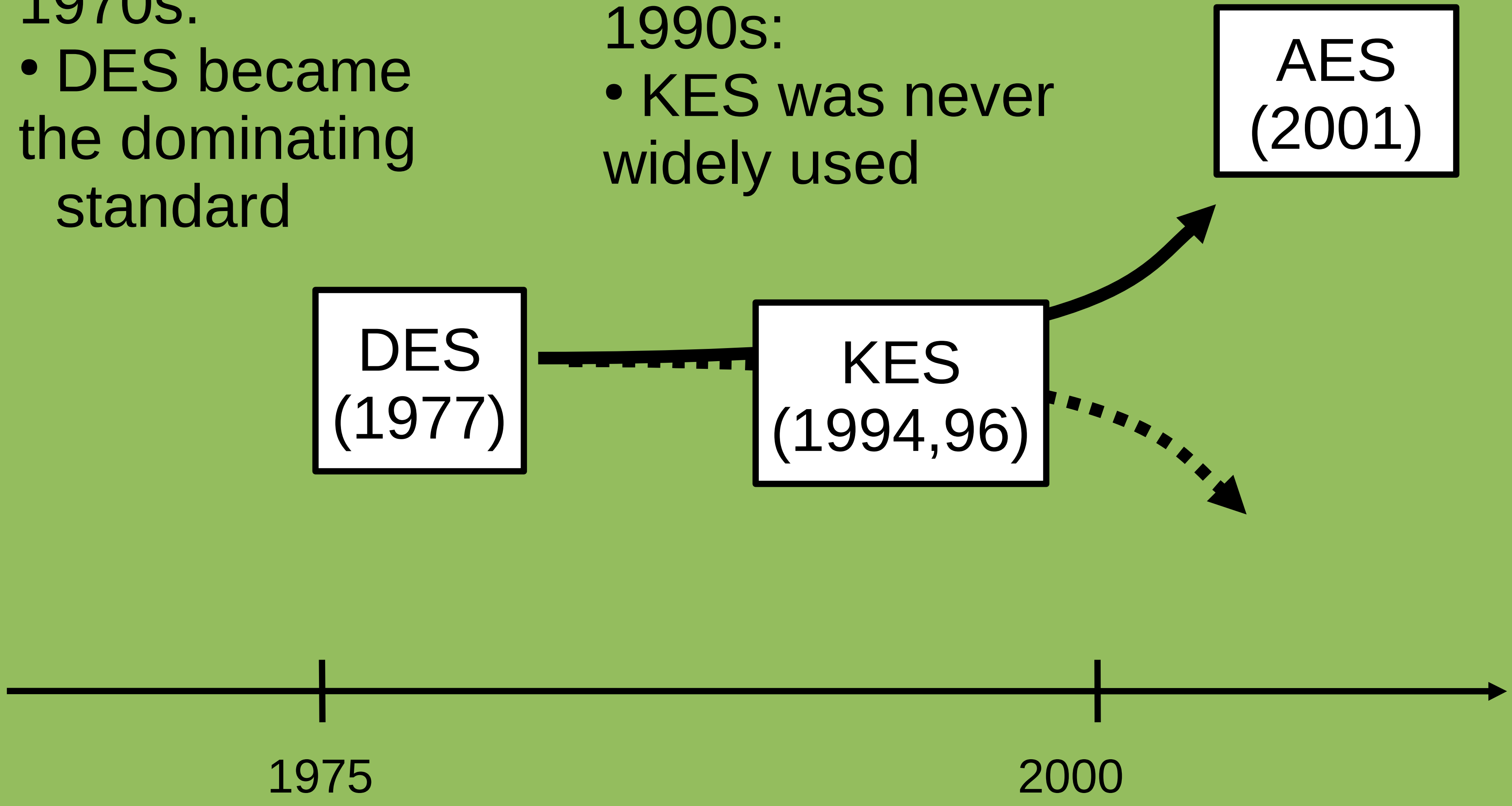
Privacy advocates:

- *“privacy of communication is a civil right”*

The artifacts of the fight

1970s:
- DES became the dominating standard

1990s:
- KES was never widely used

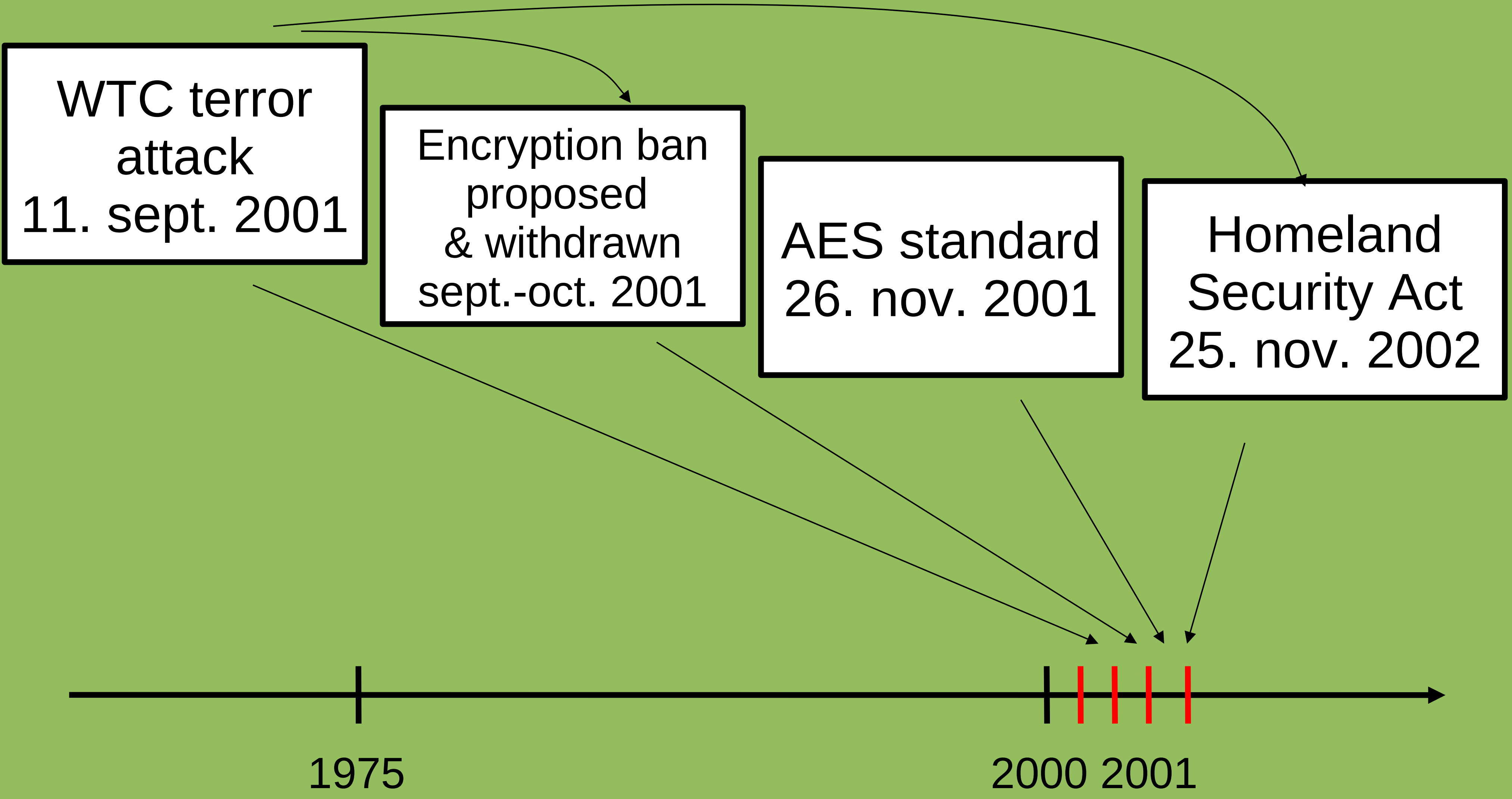


DES (1977)

KES (1994,96)

AES (2001)

The end result was not a given



WTC terror attack
11. sept. 2001

Encryption ban proposed
& withdrawn
sept.-oct. 2001

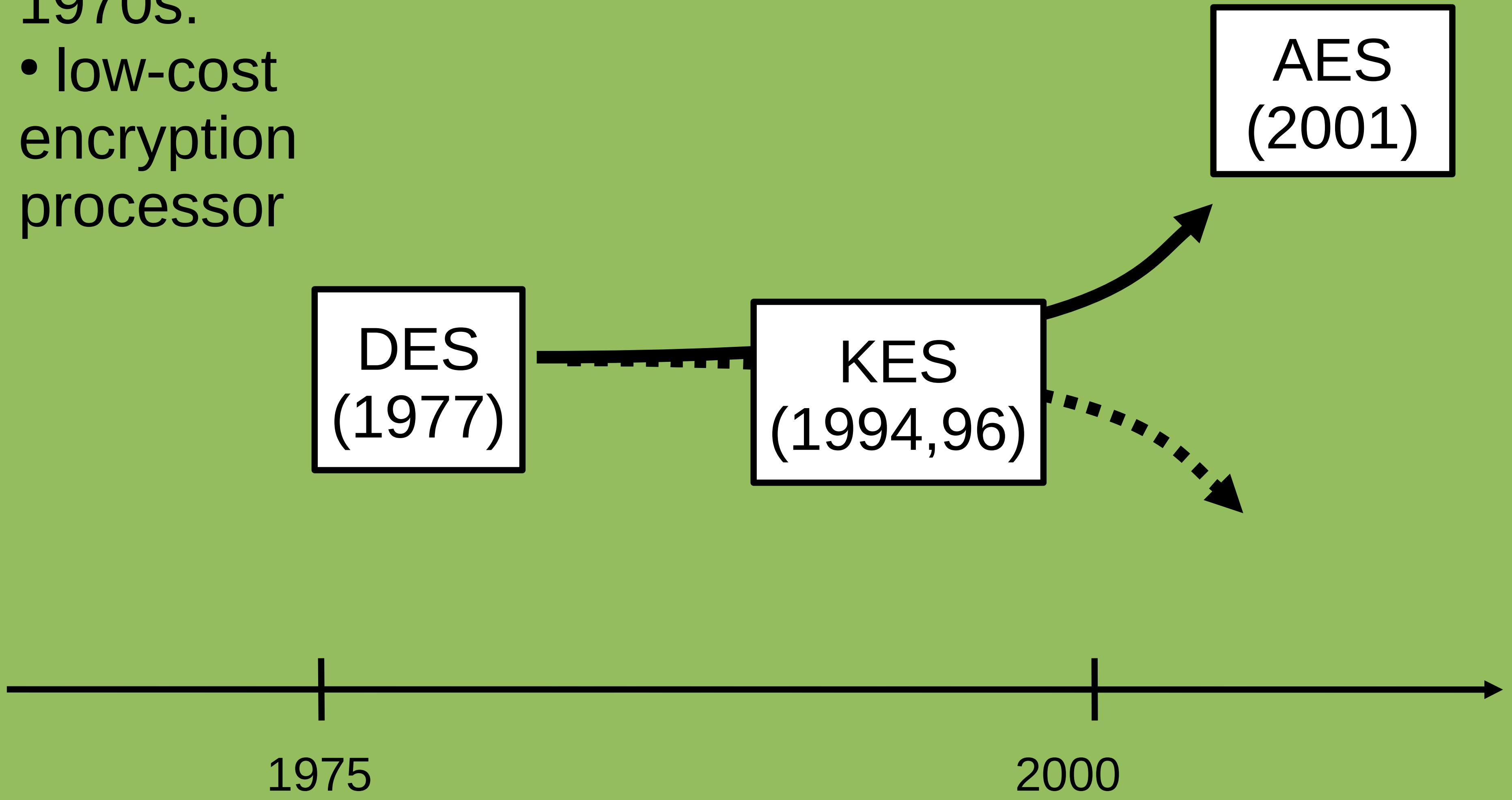
AES standard
26. nov. 2001

Homeland Security Act
25. nov. 2002

Technical feasibility

1970s:

- low-cost encryption processor



DES (1977)

KES (1994,96)

AES (2001)

1975

2000

Technical feasibility (DES)

Before DES:

Demand for encryption:

- Banks wanted to use encryption

Technical feasibility:

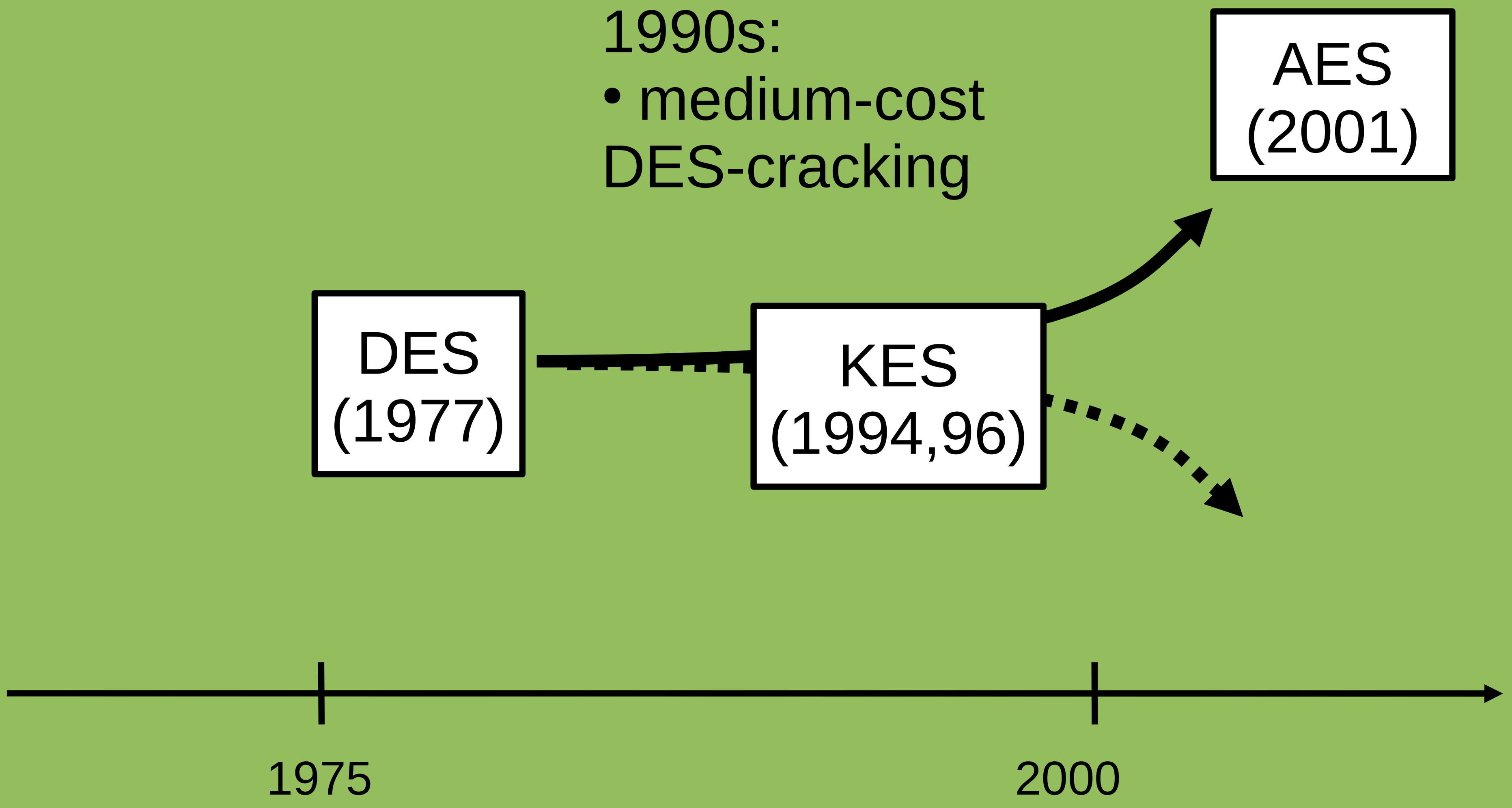
- new hardware technolog: integrated circuits
- possible to mass produce a cheap encryption chip
- hardware implementation necessary (factor ~1000 vs. software)

But there were no encryption products on the market

DES created a market

- mandatory in government
- economics of scale for vendors
- competition between vendors
- no alternatives on the market to DES's semi-strong encryption

Technical feasibility



1990s:

- medium-cost DES-cracking

DES (1977)

KES (1994,96)

AES (2001)

1975

2000

Technical feasibility: cracking of DES

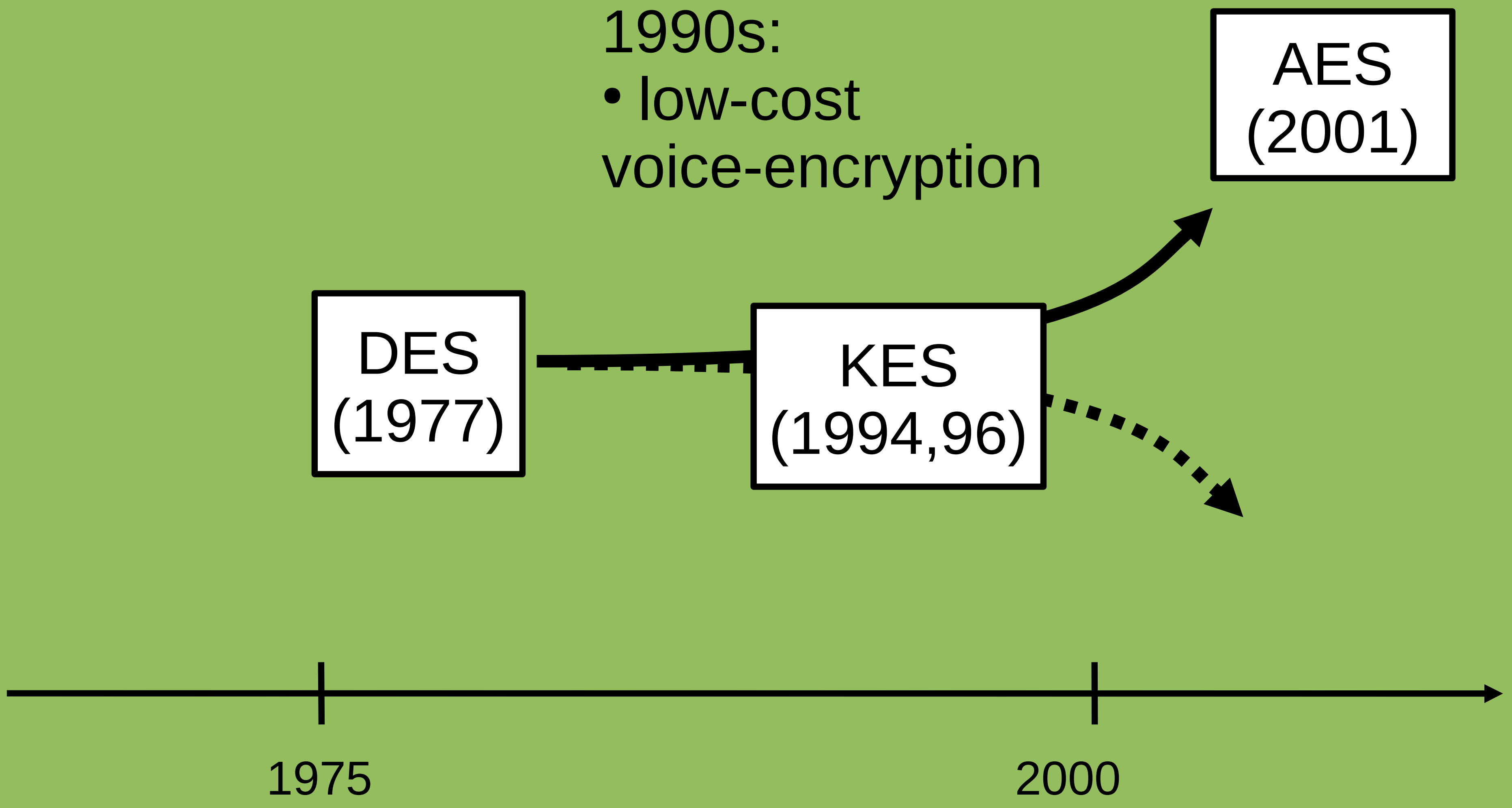
“DES-cracker” built by EFF (privacy advocates)

- broke DES in 3 days
- cost $ 1/4 mill.

DES-cracker contest

- 10.000$ prize
- by RSA Security Inc.
- ciphertext:
  - 79 45 81 c0 a0 6e 40 a2..
- plaintext:
  - “It's time for those 128-, 192-, and 256 bit keys”.

Technical feasibility



1990s:
- low-cost voice-encryption

AES (2001)

DES (1977)

KES (1994,96)

1975

2000

Key Escrow Standard (1994)

Key Escrow Standard (1994)

- by NIST
- strong encryption of phone conversation
- mandatory in government
- with a legal warrant, law enforcement agencies can get access to the encryption key

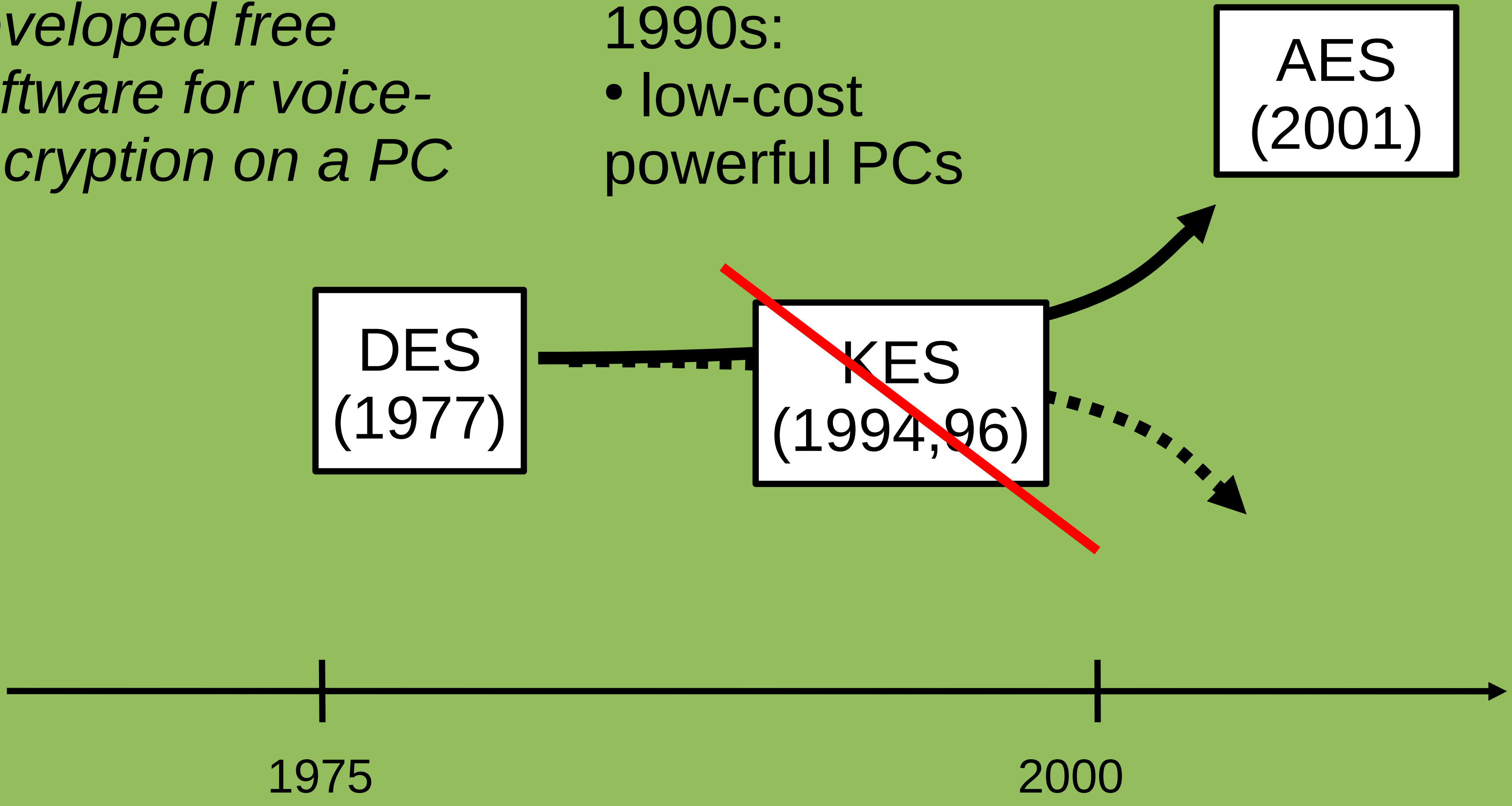
AT&T marketed model 3600

- KES compliant
- cost ~$1000
- never sold outside government

Technical feasibility: alternatives to KES

Privacy activists developed free software for voice-encryption on a PC

1990s:
- low-cost powerful PCs



DES
(1977)

~~KES
(1994,96)~~

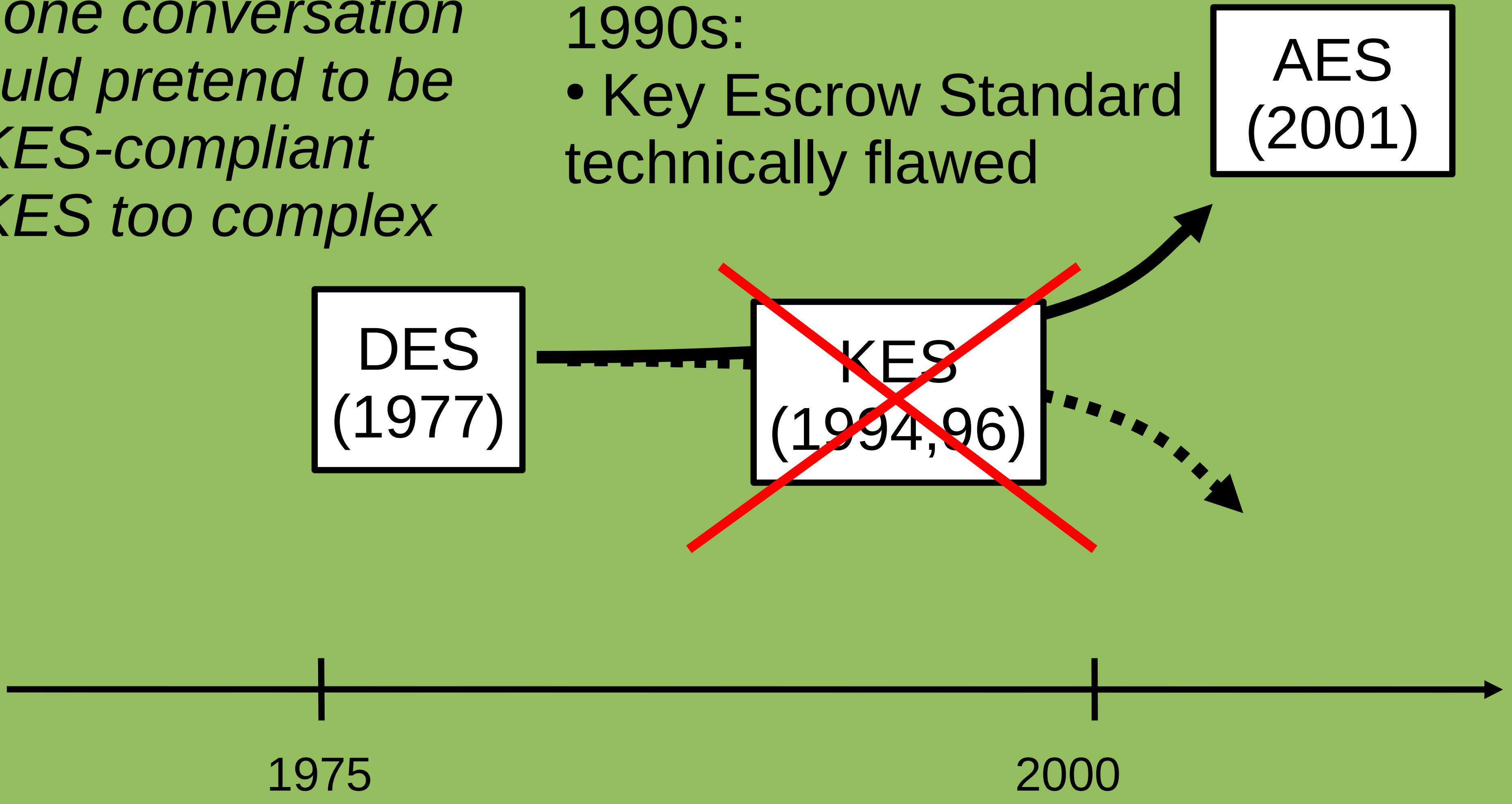
AES
(2001)

Technical infeasibility of KES

- *one party in a phone conversation could pretend to be KES-compliant*
- *KES too complex*

1990s:

- Key Escrow Standard technically flawed



Conclusion

Influence of technical developments:

1970s: chip-technology

- DES became dominant market standard

1990s: chip-technology

- DES became obsolete (broken)
- voice encryption and other new applications
- also software alternatives to government standards

1990s: complexity of network technology

- failure of Key Escrow Standard