Cryptography Basics and Symmetric Cryptography

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 2

ravi.utsa@gmail.com
www.profsandhu.com

Basic Concepts

Cryptographic Technology

SYMMETRIC KEY

Secret Key
Single Key
Conventional

ASYMMETRIC KEY

Public Key
Public-Private Key

Cryptographic Technology

- Symmetric-key encryption
- Symmetric-key message authentication codes (MACs)
- Public-key encryption
- Public-key digital signatures
- Public-key key agreement
- Message digests (hash functions)
- Public-key certificates
- Challenge-response authentication

Cryptographic Technology

- Symmetric-key encryption
- Symmetric-key message authentication codes (MAC)
- Public-key encryption
- Public-key digital signatures
- Public-key key agreement
- Message digests (hash functions)
- Public-key certificates
- Challenge-response authentication

SSL uses all of these

ATMs run on symmetric-key technology

I·C·S The Institute for Cyber Security

Cryptographic Services

UTSA

- confidentiality
  - traffic flow confidentiality
- integrity
- authentication
- non-repudiation

Traditional formulation

Cryptographic Services

- confidentiality
  - crypto keys leak profusely via side channels
- integrity + authentication
  - no point having one without the other
- non-repudiation
  - requires asymmetric cryptography
  - stronger form of integrity + authentication
- replay protection
  - beyond integrity?

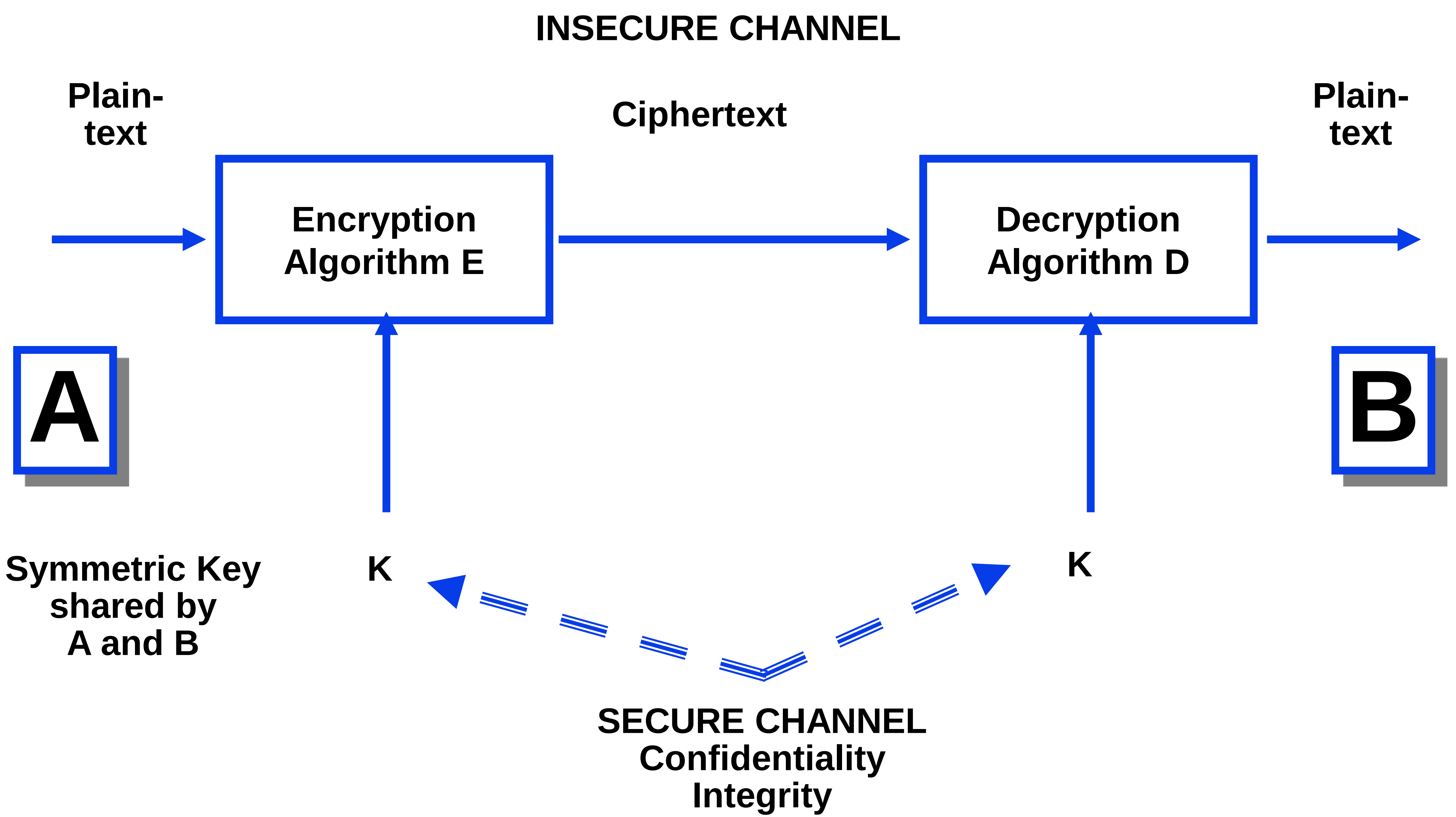
Important insights

Safe Cryptography

- Symmetric-key cryptography
  - 128 bit or higher
- Public-key cryptography
  - 2048 bit or higher
- Message digests
  - 256 bit or higher
- These numbers keep increasing
  - https://www.keylength.com/

Symmetric Encryption

Symmetric-Key Encryption



Symmetric-Key Encryption

- confidentiality depends only on secrecy of the key
  - size of key is critical
- Symmetric key systems do not scale well
  - with N parties we need to generate and distribute N*(N-1)/2 keys
- A and B can be people or computers

Master Keys and Session Keys

- master keys, long lifetime
  - prolonged use increases exposure
- session keys
  - short-term keys communicated by means of
    - master symmetric keys
    - public key technology

Cryptanalysis

- ciphertext only
  - cryptanalyst only knows ciphertext
- known plaintext
  - cryptanalyst knows some plaintext-ciphertext pairs
- chosen plaintext
- chosen ciphertext

Known-Plaintext Attack

- 40 bit key requires $2^{39} \approx 5 * 10^{11}$ trials on average (exportable from USA, early 1990's)
- trials/second time required

1	20,000 years
10^3	20 years
10^6	6 days
10^9	9 minutes
10^{12}	0.5 seconds

Known-Plaintext Attack

- 56 bit key requires $2^{55} \approx 3.6 * 10^{\wedge 16}$ trials on average (DES, 1977)
- trials/second time required

1	10^9 years
10^3	10^6 years
10^6	10^3 years
10^9	1 year
10^{12}	10 hours

Known-Plaintext Attack

- 80 bit key requires $2^{79} \approx 6 * 10^{23}$ trials on average (SKIPJACK, mid-1990s)
- trials/second time required

1	10^{16} years
10^{3}	10^{13} years
10^{6}	10^{10} years
10^{9}	10^{7} years
10^{12}	10^{4} years

Known-Plaintext Attack

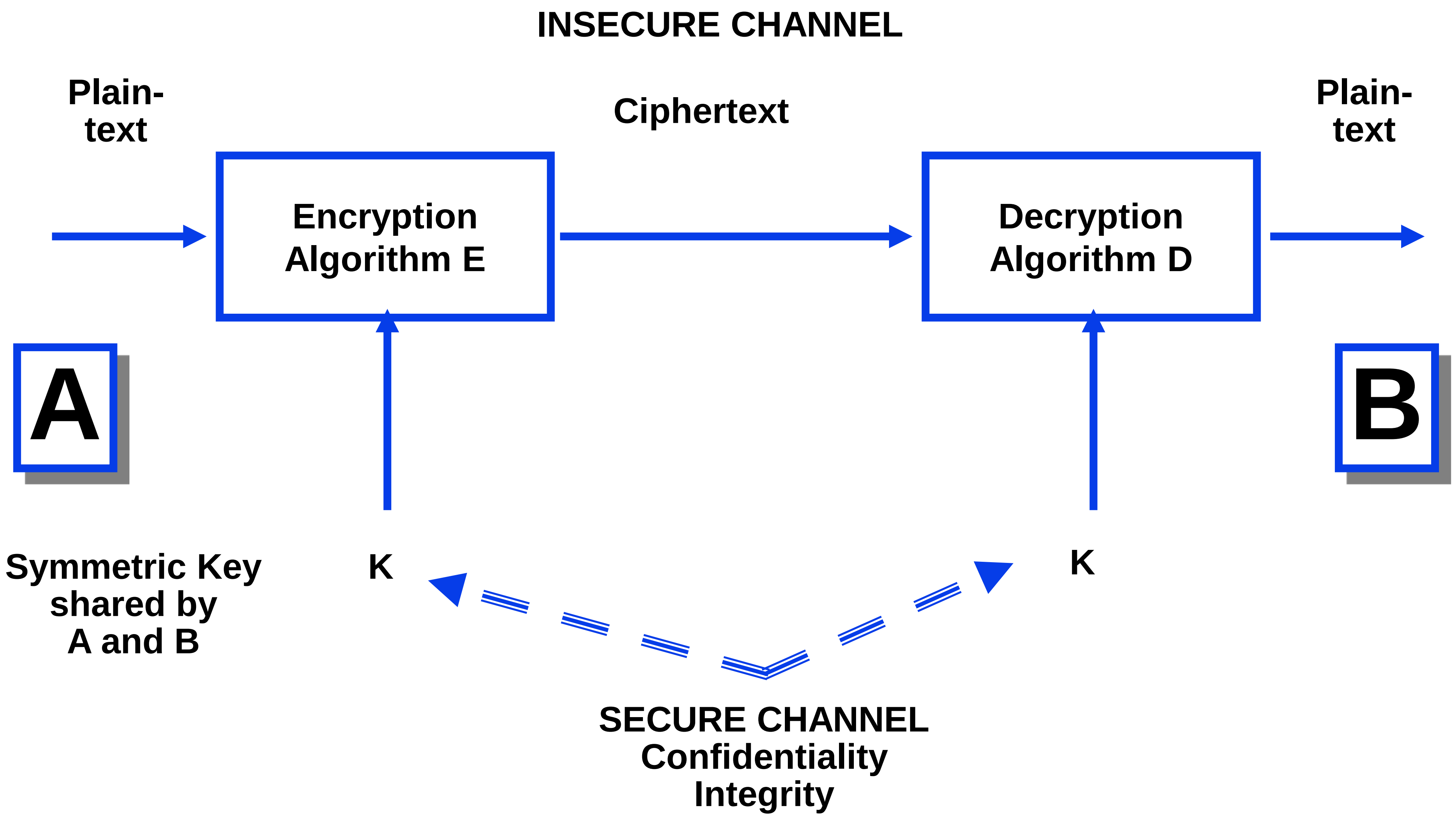
- 128 bit key requires $2^{127} \approx 2 * 10^{38}$ trials on average (AES-128, 2001)
- trials/second time required

1	10^{30} years
10^{3}	10^{27} years
10^{6}	10^{24} years
10^{9}	10^{21} years
10^{12}	10^{18} years

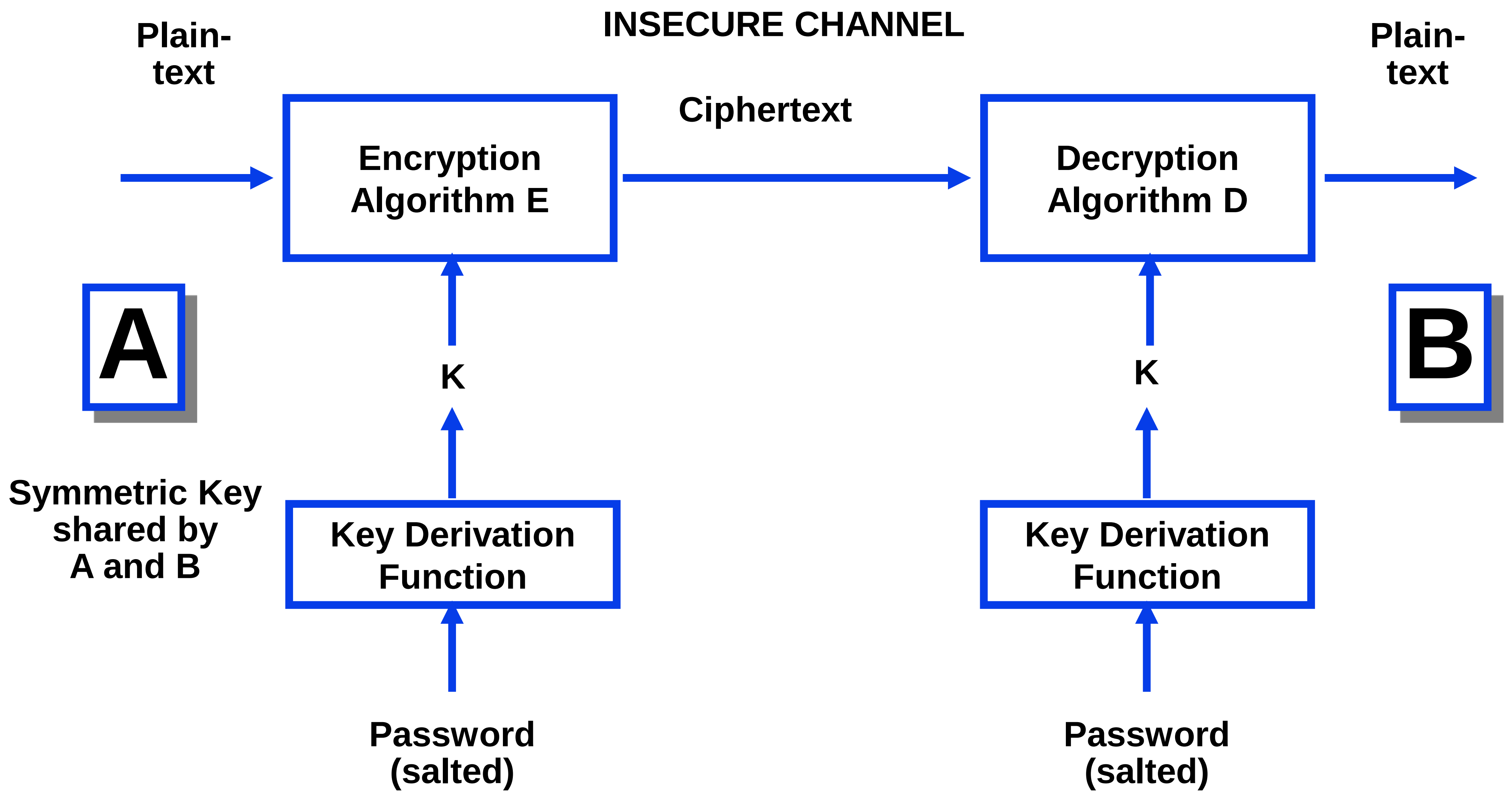
AES

- Advanced encryption standard, 2001
  - DES, 1977: designed by IBM. Blessed by NSA.
  - SKIPJACK, early 1990s: designed by NSA, declassified 1998
  - AES, 2001: designed by open international competition, winner was a European team
- 3 key sizes: 128, 192, 256
- Block size: 128
  - Previously most (e.g. DES) used 64 bit block size
  - 128 bit block size is safer due to birthday attack

Symmetric-Key Encryption

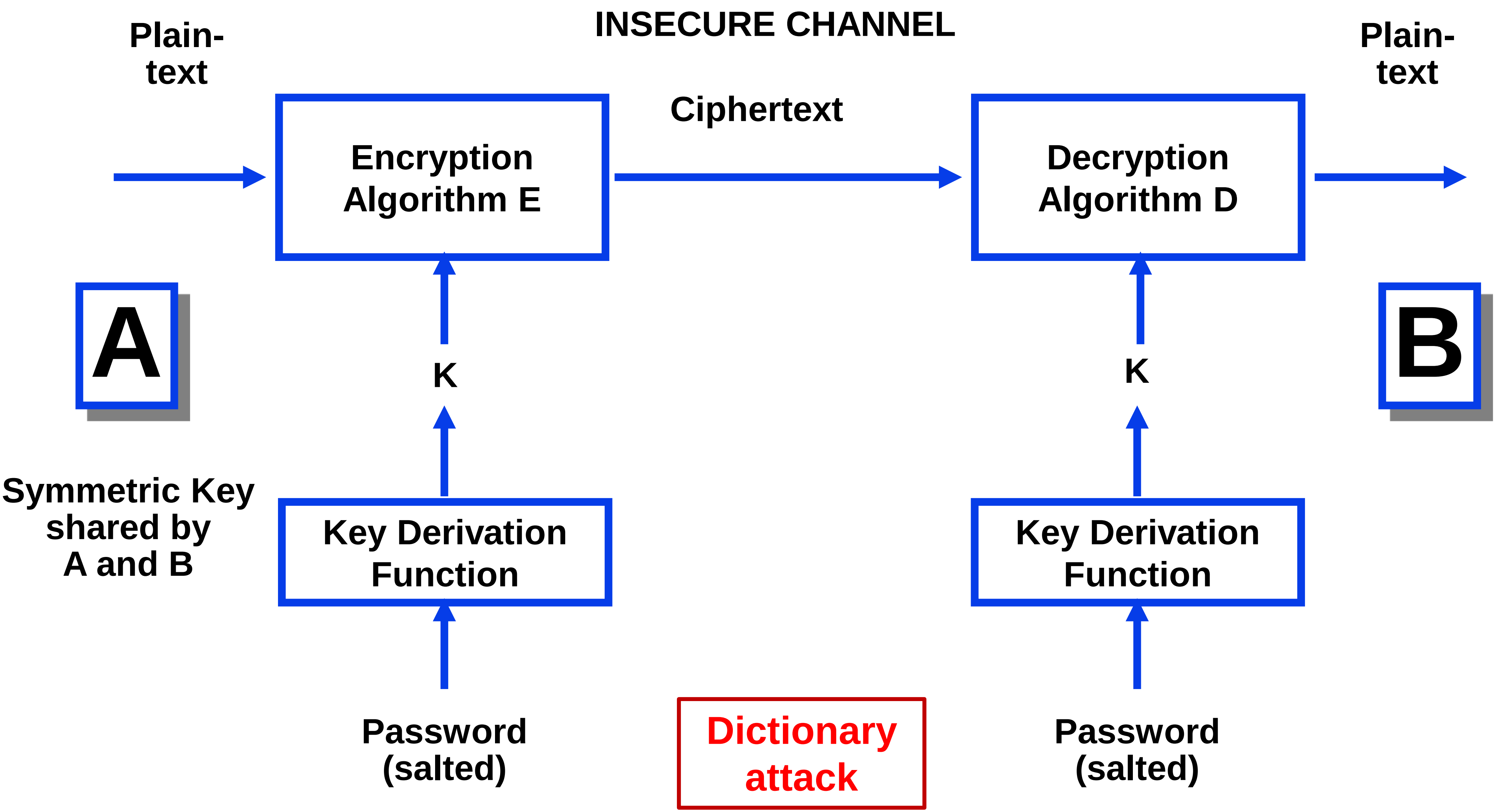


Password Derived Keys

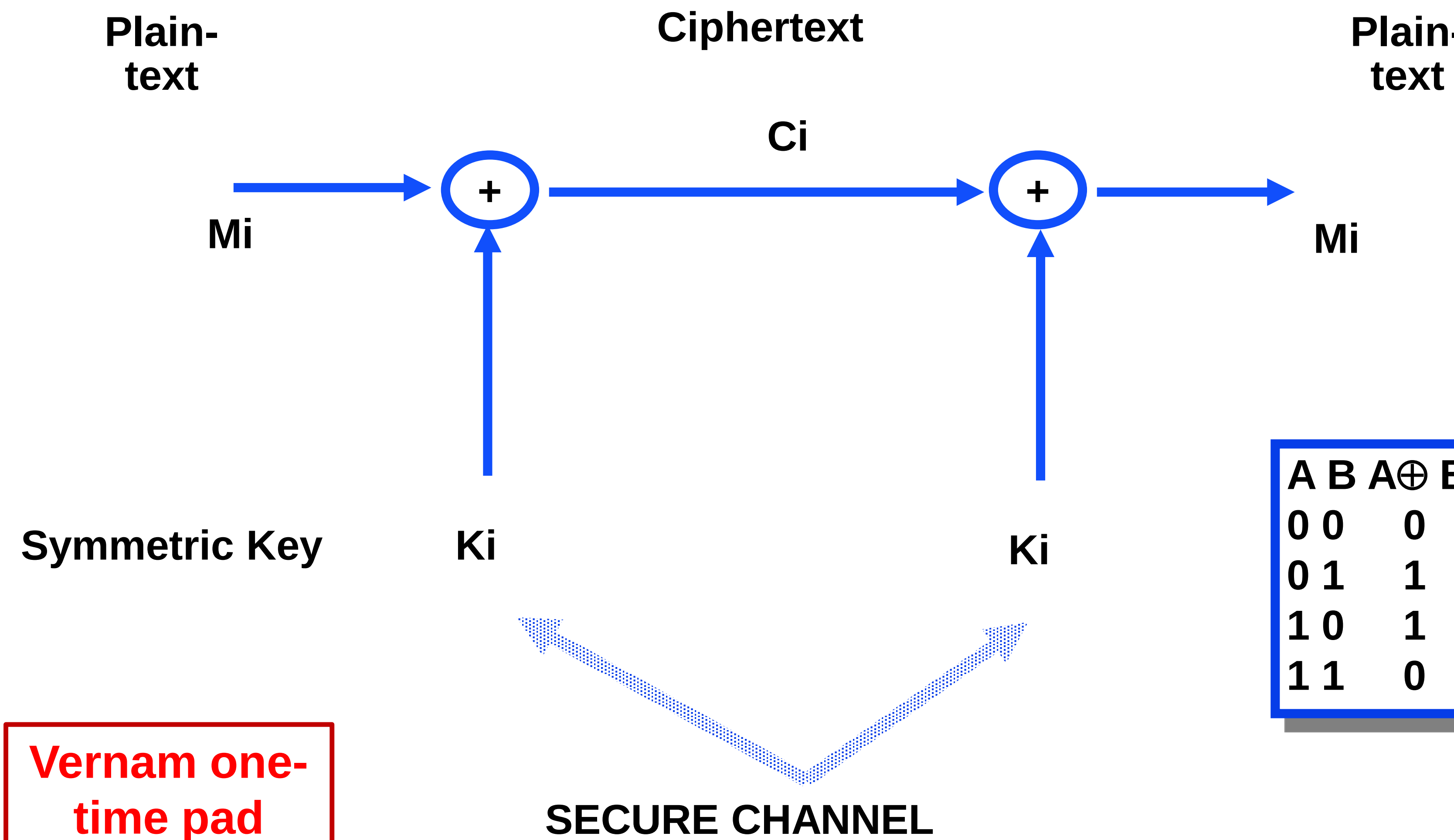


World-Leading Research with Real-World Impact!

Password Derived Keys



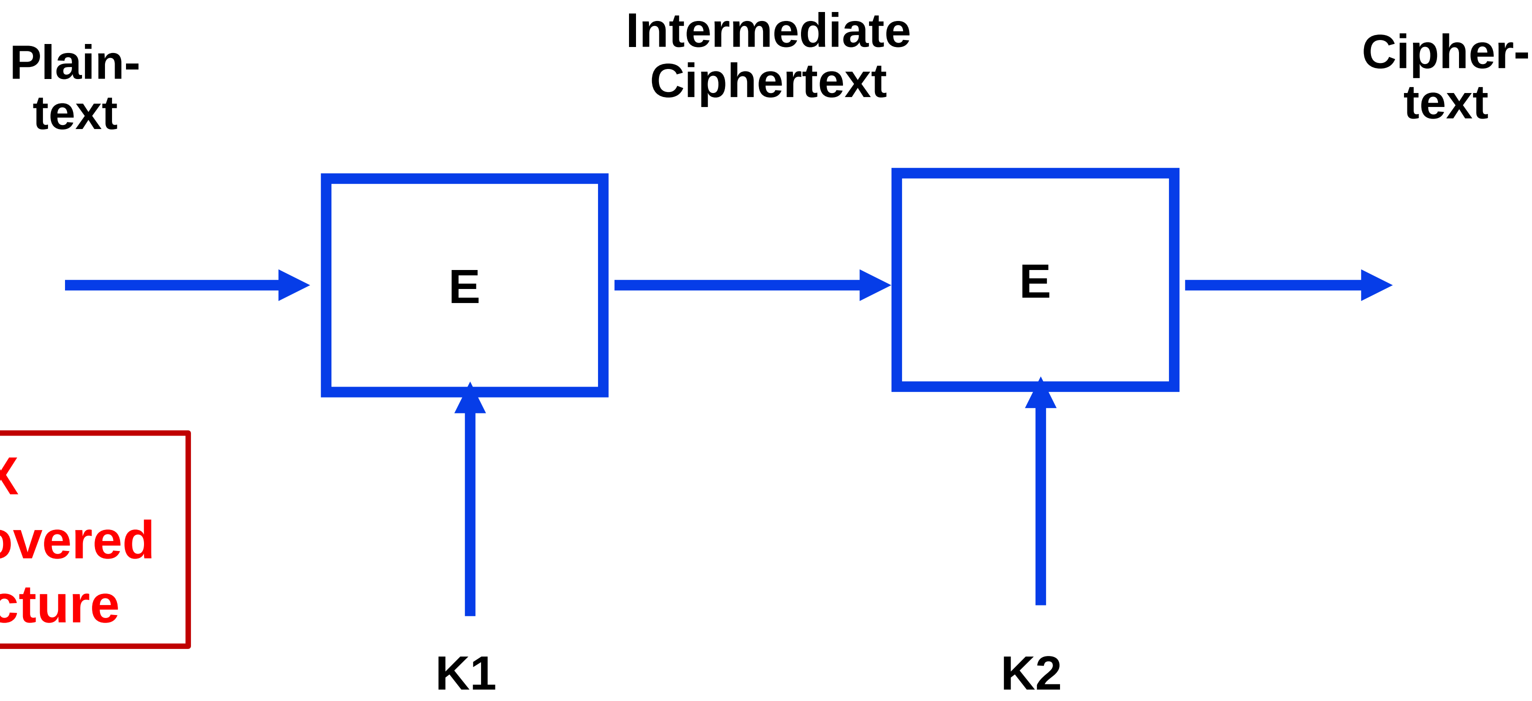
Perfect Secrecy



A	B	A⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Vernam one-time pad

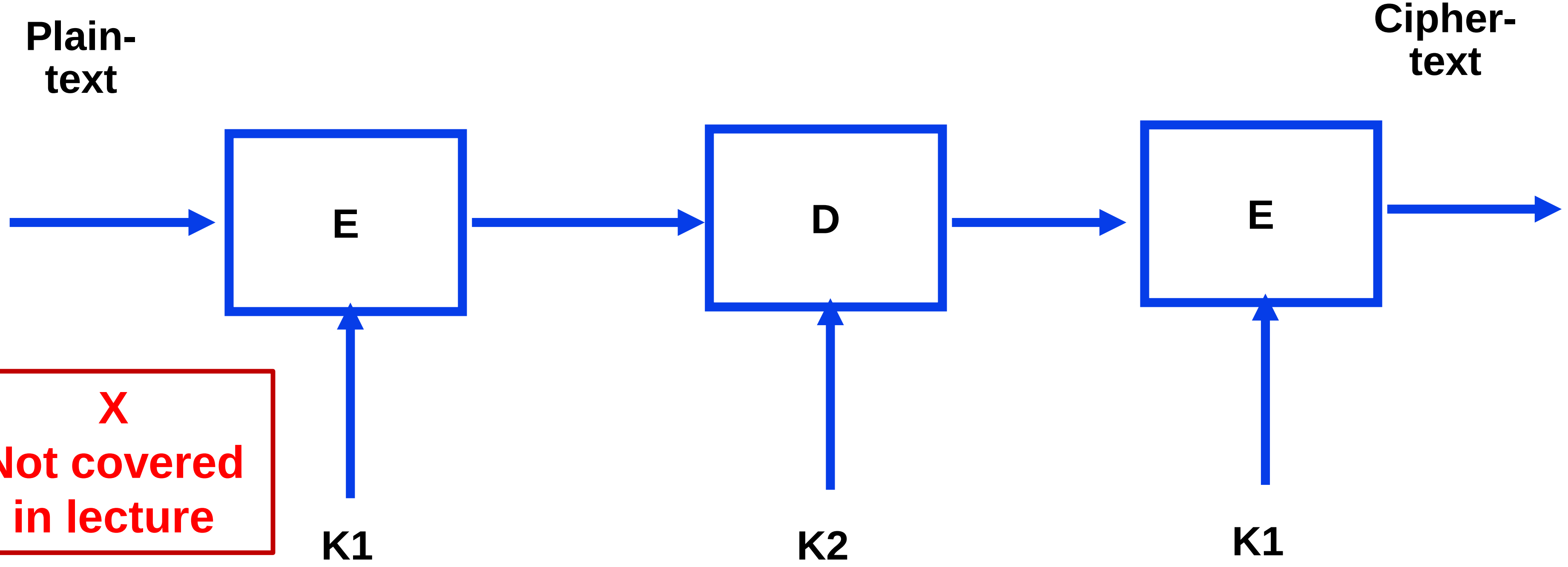
Double DES



X
Not covered
in lecture

- effective key size is only 57 bits due to meet-in-the-middle attack

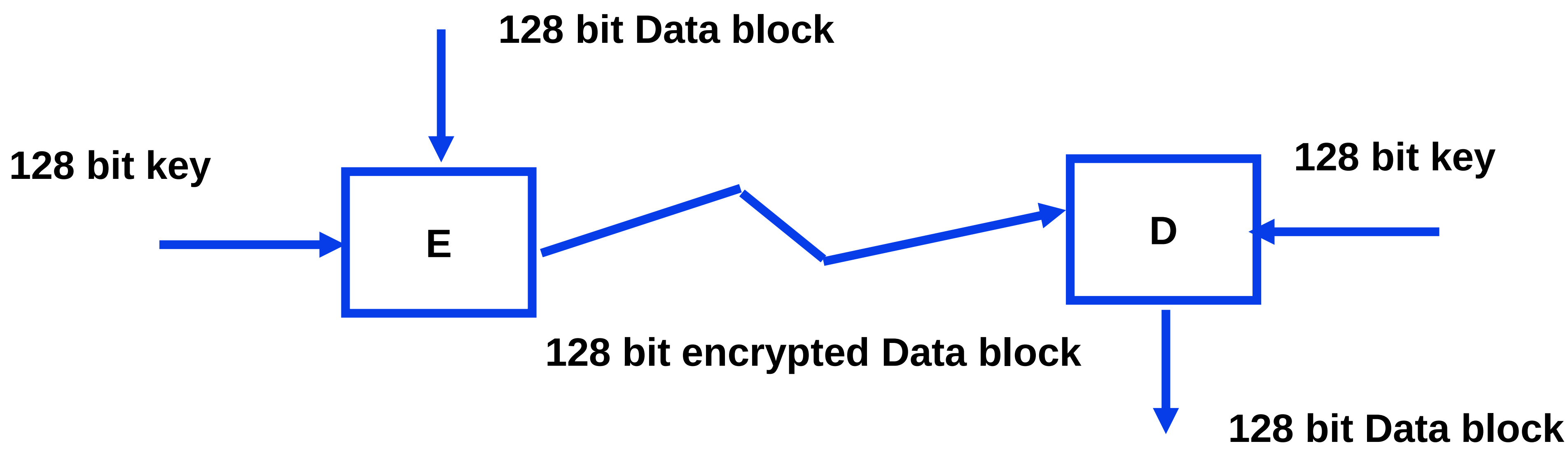
Triple DES



X
Not covered
in lecture

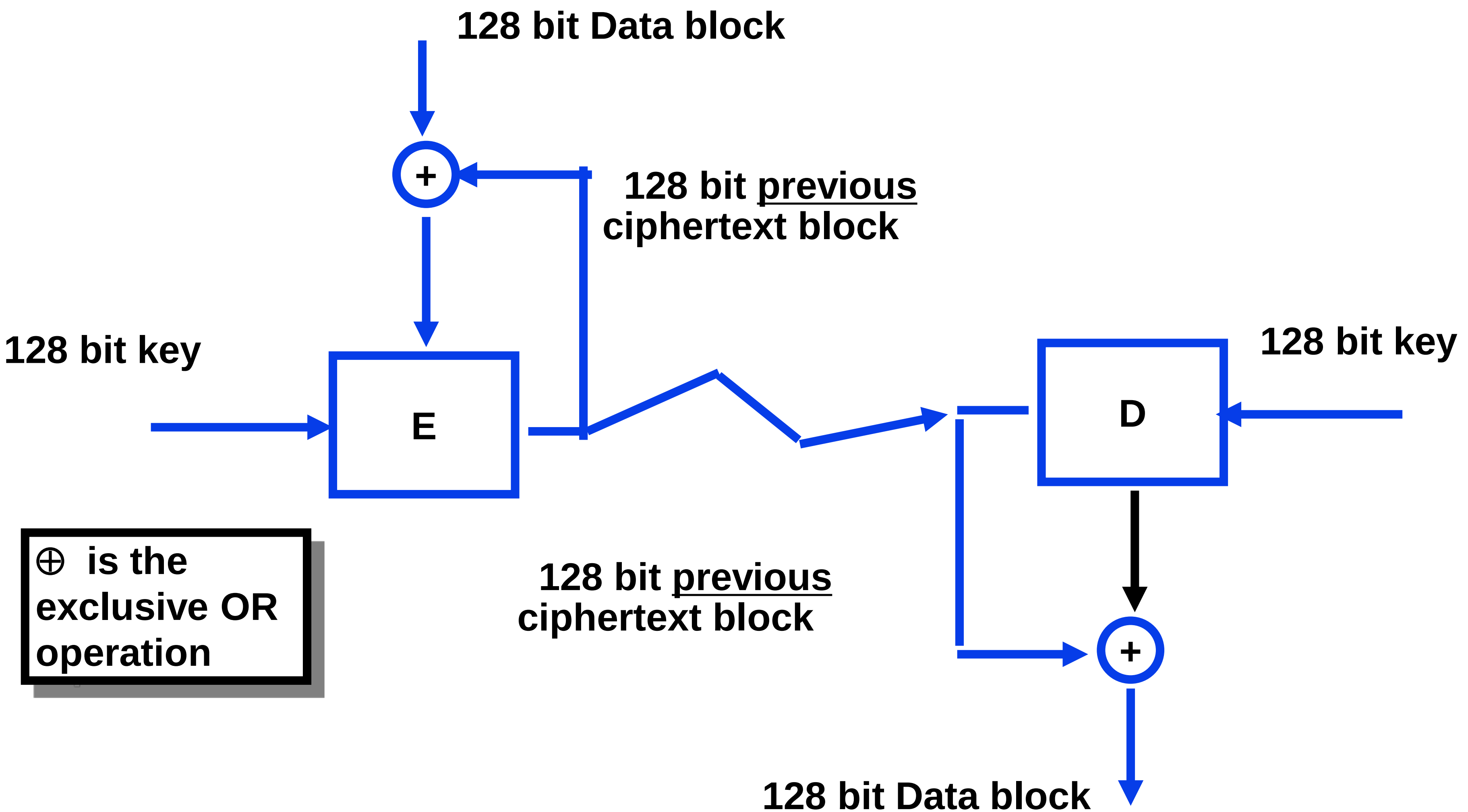
- effective key size is 112 bits due to meet-in-the-middle attack

Electronic Code Book (ECB) Mode



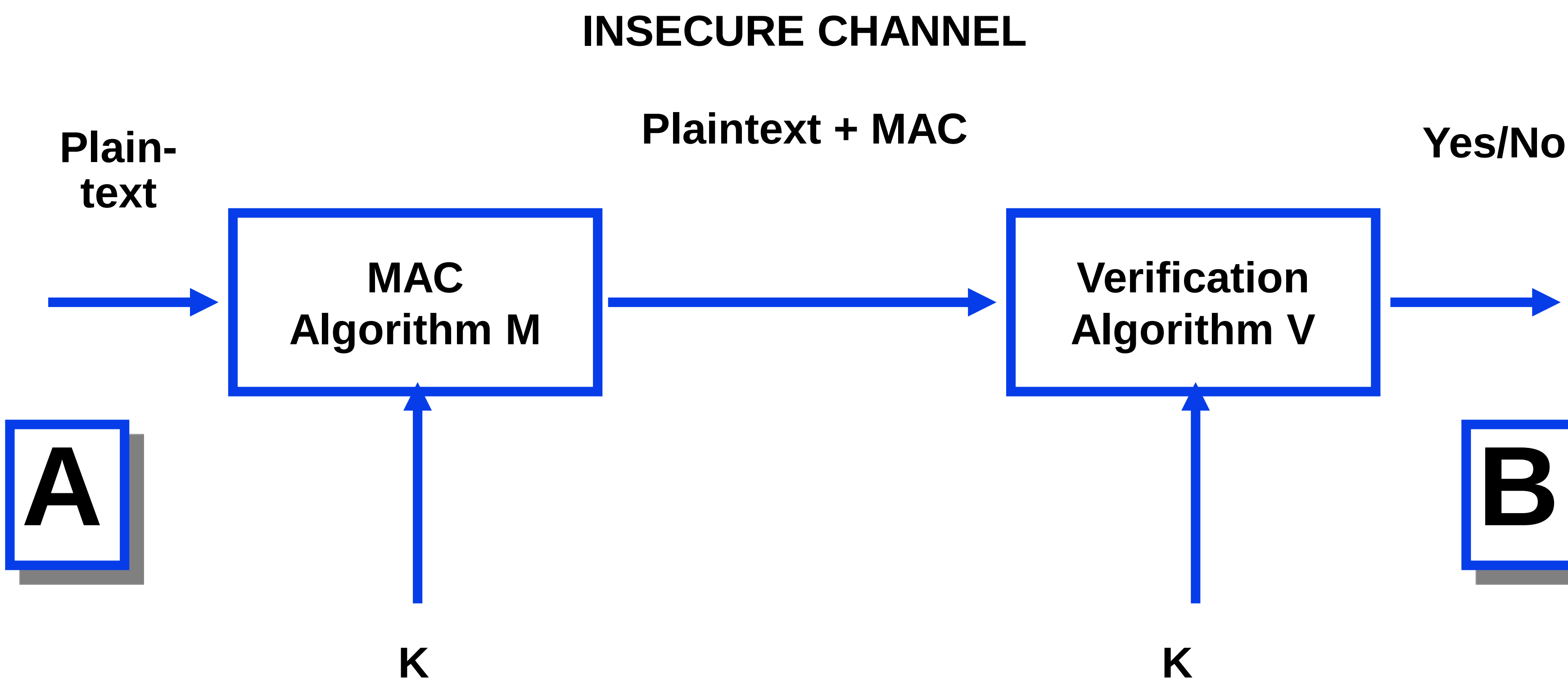
- OK for small messages
- identical data blocks will be identically encrypted

Cipher Block Chaining (CBC) Mode

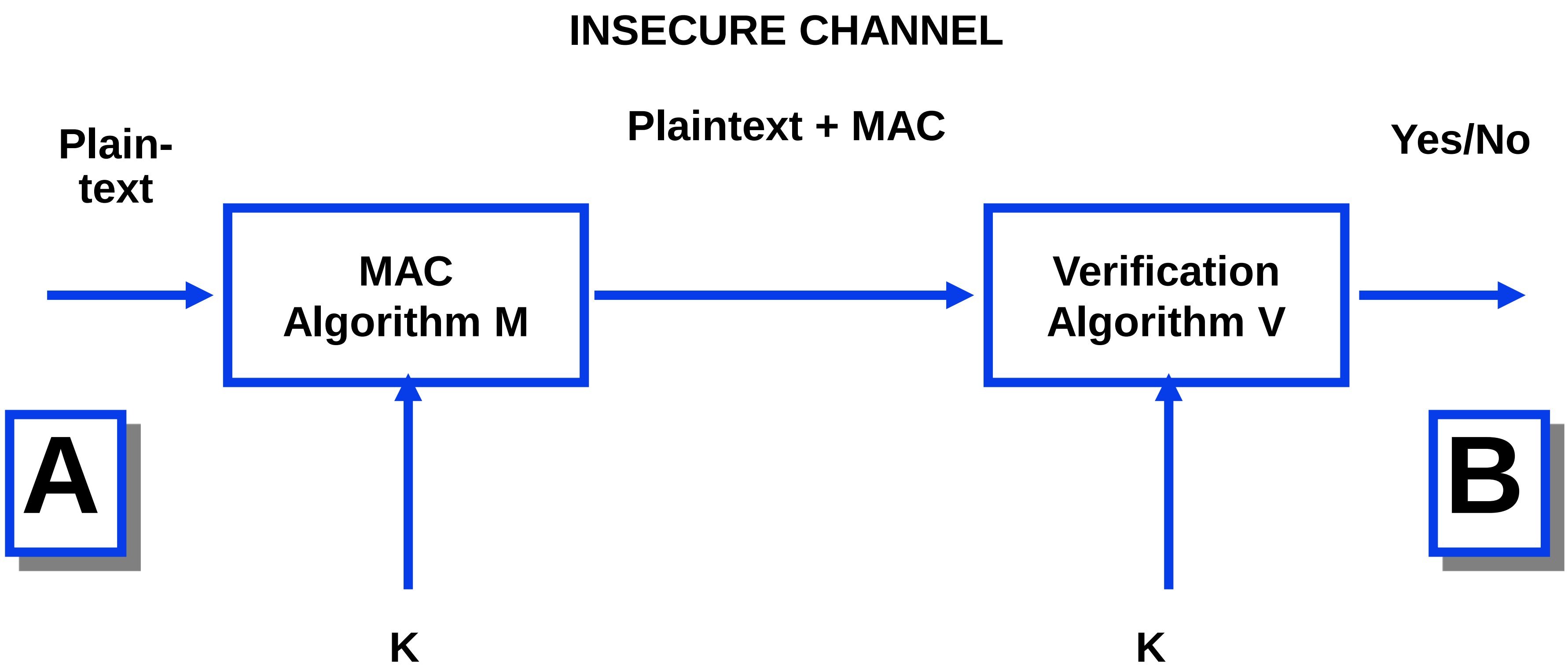


Symmetric-Key Message Authentication Code (MAC)

Message Authentication Code



Message Authentication Code



Does not provide non-repudiation

Message Authentication Code

Symmetric Encryption Based

Message-Digest Based

Message Authentication Code

Symmetric Encryption Based

Message-Digest Based

Will revisit after discussing message digests