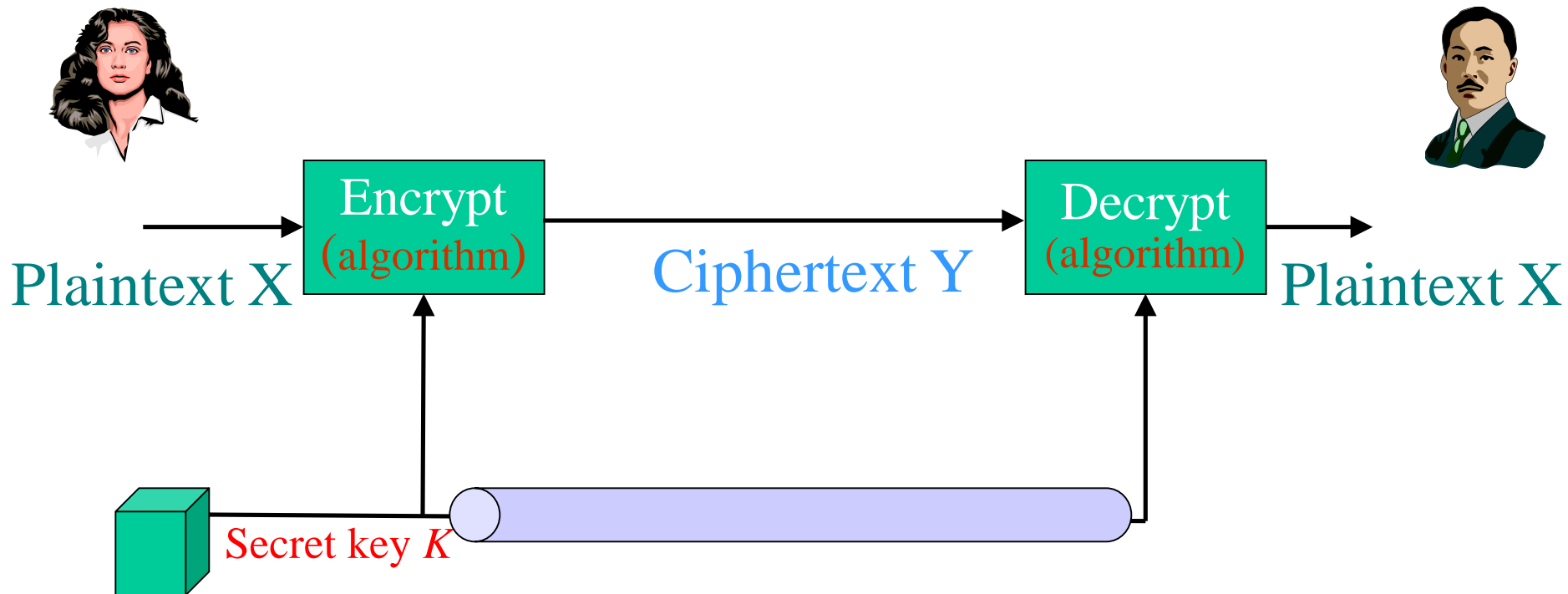

Introduction to Symmetric Cryptography

Tingting Chen
Cal Poly Pomona

Basic Cryptography

- Private Key Cryptography
 - Secret Key Cryptography, Symmetric Cryptography, Classical Cryptography
- Public Key Cryptography

Classical Cryptography



Classical Cryptography

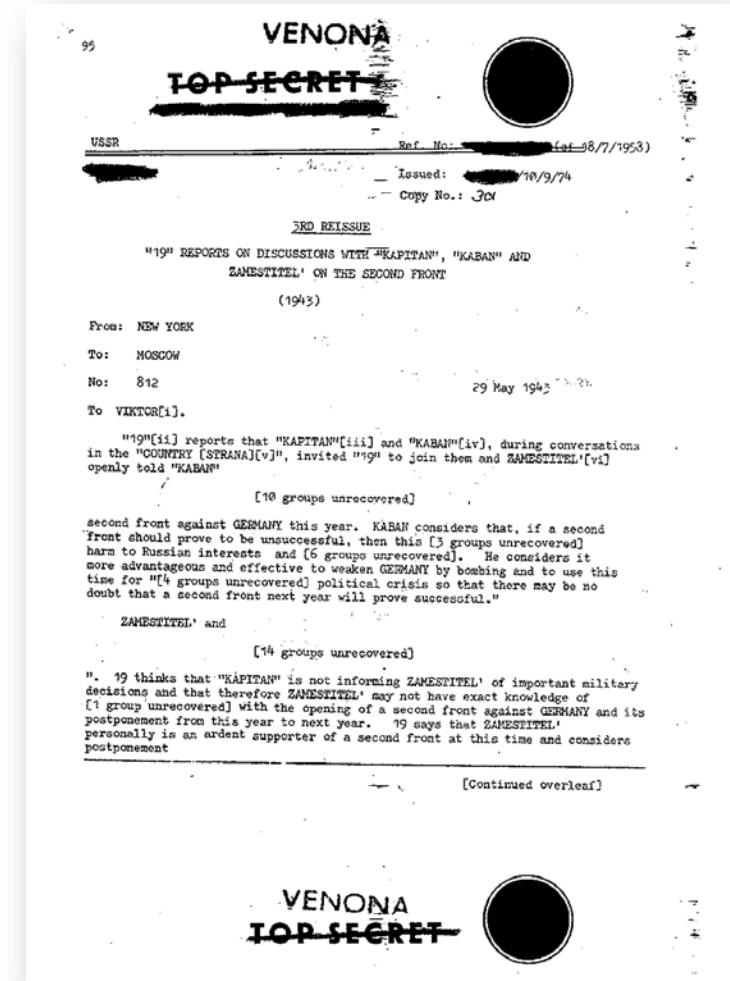
- Sender, receiver share common key
 - Keys may be the same, or trivial to derive from one another
- Two basic types
 - Transposition ciphers
 - Substitution ciphers
 - e.g., Caesar cipher, Vigenere cipher, one-time pad, S-box

One-Time Pads

- There is one type of substitution cipher that is absolutely unbreakable.
 - The **one-time pad** was invented in 1917 by Joseph Mauborgne and Gilbert Vernam
 - We use a block of shift keys, (k_1, k_2, \dots, k_n) , to encrypt a plaintext, M , of length n , with each shift key being chosen uniformly at random.
- Since each shift is random, every ciphertext is equally likely for any plaintext.

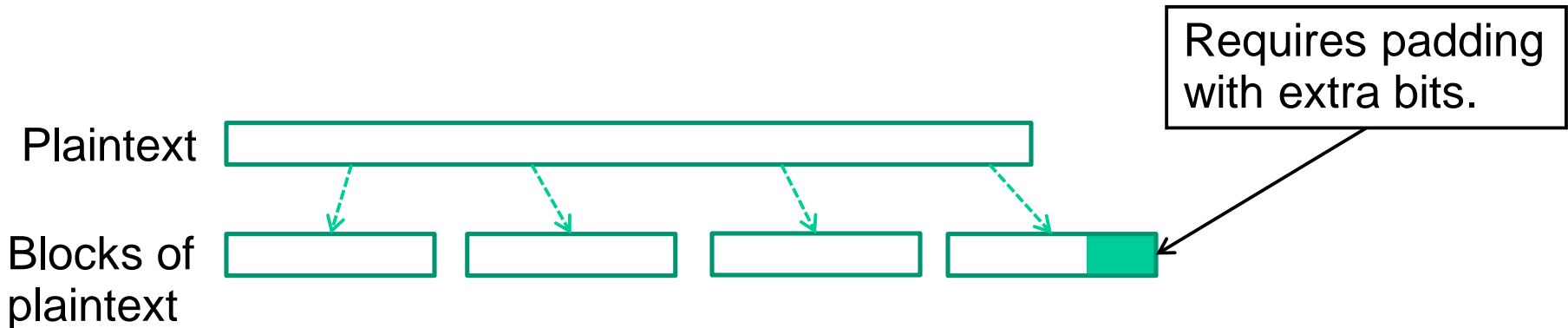
Weaknesses of the One-Time Pad

- In spite of their perfect security, one-time pads have some weaknesses
- The key has to be as long as the plaintext
- Keys can never be reused
 - Repeated use of one-time pads allowed the U.S. to break some of the communications of Soviet spies during the Cold War.



Block Ciphers

- In a **block cipher**:
 - Plaintext and ciphertext have fixed length b (e.g., 128 bits)
 - A plaintext of length n is partitioned into a sequence of m **blocks**, $P[0], \dots, P[m-1]$, where $n \leq bm < n + b$
- Each message is divided into a sequence of blocks and encrypted or decrypted in terms of its blocks.

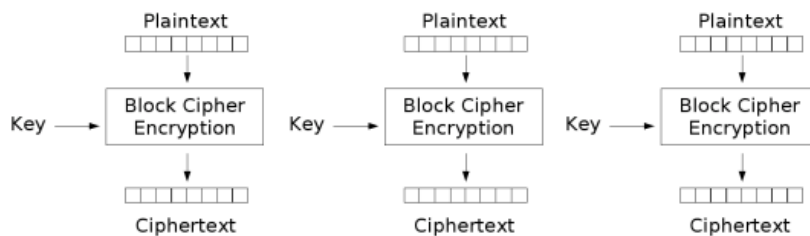


Block Ciphers in Practice

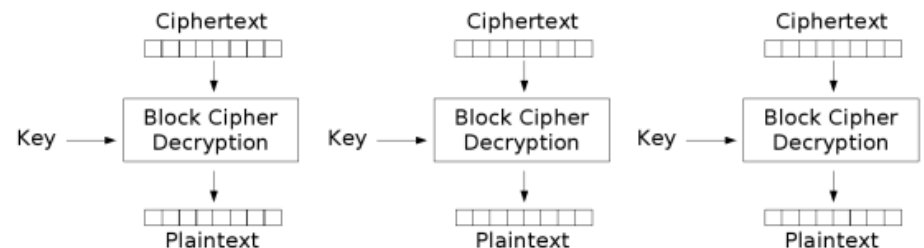
- Data Encryption Standard (DES)
 - Developed by IBM and adopted by NIST in 1977
 - 64-bit blocks and 56-bit keys
 - Small key space makes exhaustive search attack feasible since late 90s
- Triple DES (3DES)
 - Nested application of DES with three different keys K_A , K_B , and K_C
 - Effective key length is 168 bits, making exhaustive search attacks unfeasible
 - $C = E_{K_C}(D_{K_B}(E_{K_A}(P)))$; $P = D_{K_A}(E_{K_B}(D_{K_C}(C)))$
 - Equivalent to DES when $K_A=K_B=K_C$ (backward compatible)
- Advanced Encryption Standard (AES)
 - Selected by NIST in 2001 through open international competition and public discussion
 - 128-bit blocks and several possible key lengths: 128, 192 and 256 bits
 - Exhaustive search attack not currently possible
 - AES-256 is the symmetric encryption algorithm of choice

Block Cipher Modes

- A block cipher mode describes the way a block cipher encrypts and decrypts a sequence of message blocks.
- Electronic Code Book (ECB) Mode (is the simplest):
 - Block $P[i]$ encrypted into ciphertext block $C[i] = E_K(P[i])$
 - Block $C[i]$ decrypted into plaintext block $M[i] = D_K(C[i])$



Electronic Codebook (ECB) mode encryption

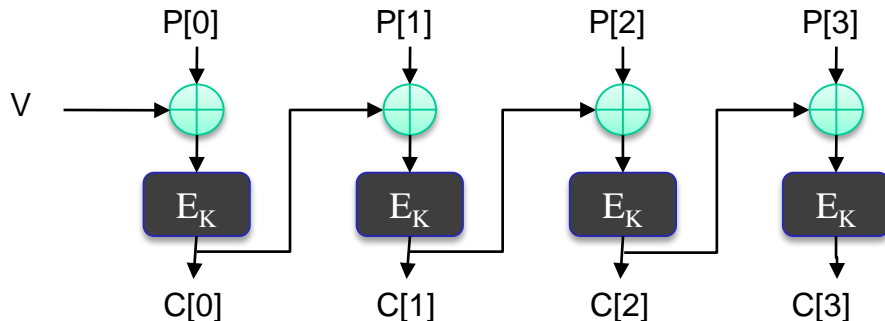


Electronic Codebook (ECB) mode decryption

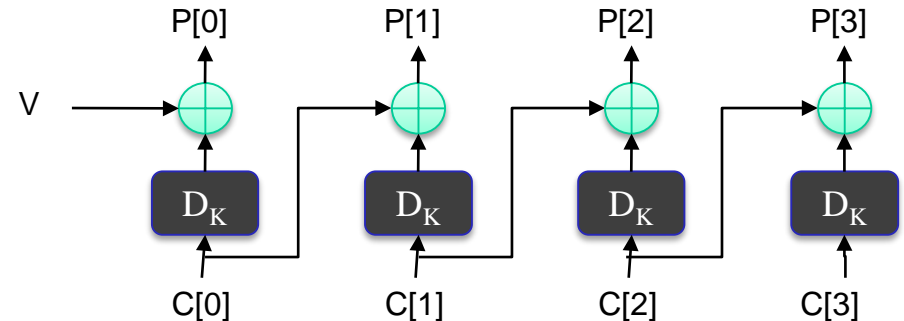
Cipher Block Chaining (CBC) Mode

- In Cipher Block Chaining (CBC) Mode
 - The previous ciphertext block is combined with the current plaintext block $C[i] = E_K (C[i - 1] \oplus P[i])$
 - $C[-1] = V$, a random block separately transmitted encrypted (known as the initialization vector)
 - Decryption: $P[i] = C[i - 1] \oplus D_K (C[i])$

CBC Encryption:



CBC Decryption:



Stream Cipher

- Key stream
 - Pseudo-random sequence of bits $S = S[0], S[1], S[2], \dots$
 - Can be generated on-line one bit (or byte) at the time
- Stream cipher
 - XOR the plaintext with the key stream $C[i] = S[i] \oplus P[i]$
 - Suitable for plaintext of arbitrary length generated on the fly, e.g., media stream

Applications of Symmetric Ciphers

- Data encryption
 - Most data is encrypted using symmetric algorithms
 - RSA encryption in Java SE
- Message Authentication Code
 - CBC-MAC
- Hash Functions based on Block Ciphers
 - One-way compression function.