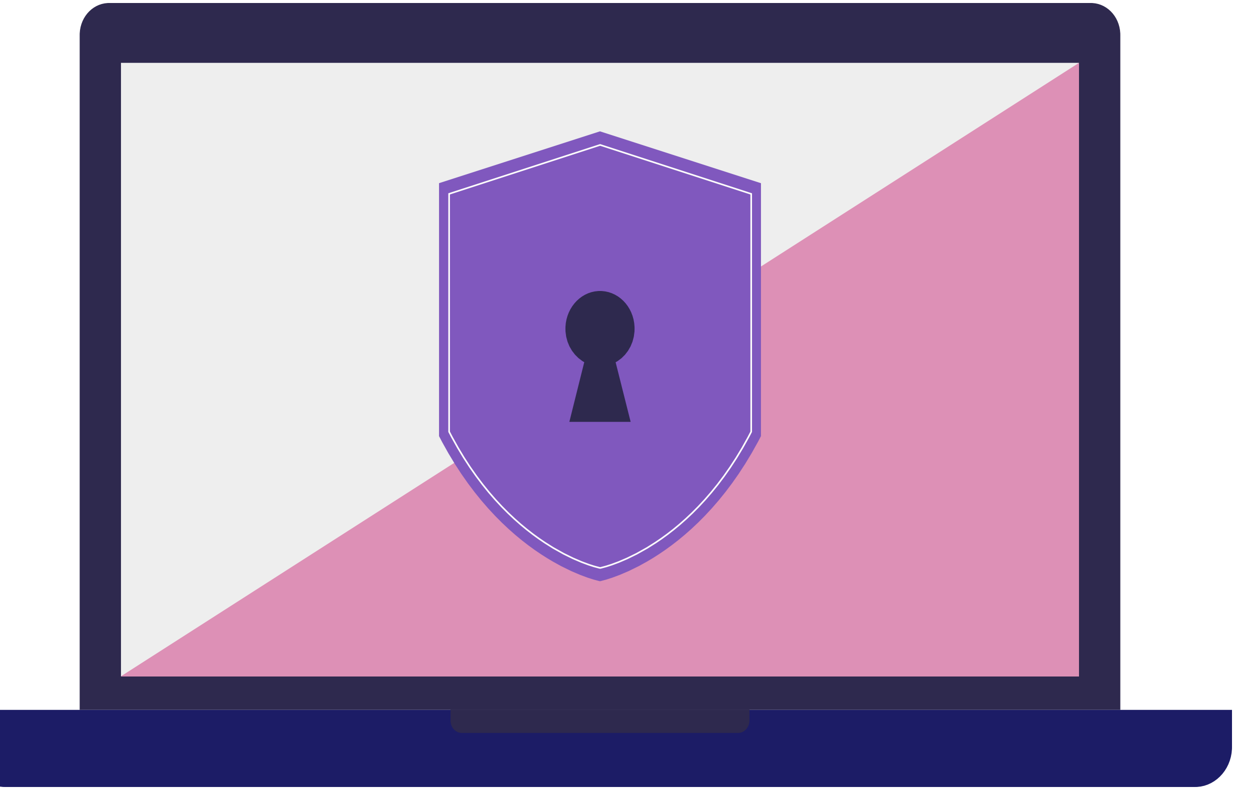
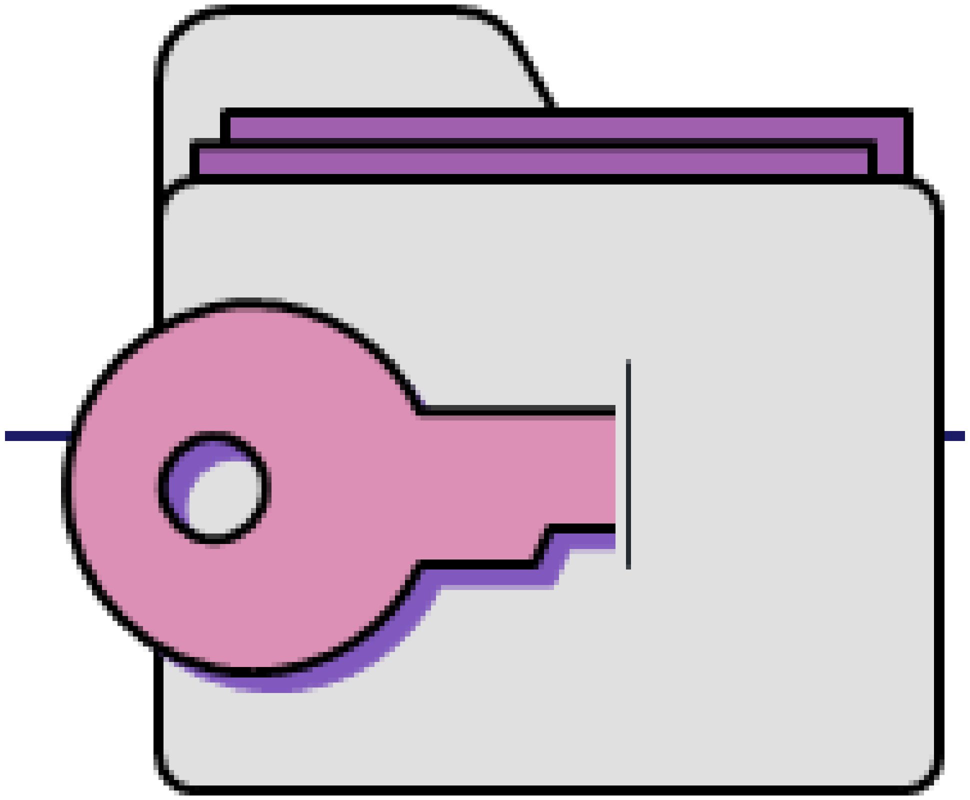


Computer Security

CS433



Chapter 12
Cryptography

Objectives

Learn	Learn basic terms and primitives of cryptography
Deep dive	Deep dive into how symmetric encryption algorithms work
Study	Study the RSA asymmetric encryption algorithm
Compare	Compare message digest algorithms
Explain	Explain the math behind digital signatures
Learn	Learn the concepts behind quantum cryptography

Methods of Cryptanalysis

Cryptanalysis is the act of studying a cryptographic algorithm, its implementation, plaintext, ciphertext, and any other available information to try to break the protection of encryption

Cryptanalyst can attempt to do …

- ✓ **Break** (decrypt) a single message
- ✓ **Recognize patterns** in encrypted messages
- ✓ **Infer some meaning** without even breaking the encryption, such as from the length or frequency of messages
- ✓ **Easily deduce the key** to break one message and perhaps subsequent ones
- ✓ **Find weaknesses** in the implementation or environment of use of **encryption by the sender**
- ✓ **Find general weaknesses** in an encryption algorithm

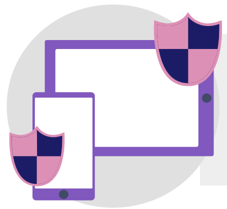
Cryptanalysis Inputs

Attack models for the cryptanalysis

- **Ciphertext only**
  - Look for patterns, similarities, and discontinuities among many messages that are encrypted alike

- **Plaintext and ciphertext**, so the cryptanalyst can see what transformations occurred
  - *Known plaintext*—the analyst has an exact copy of the plaintext and ciphertext
  - *Probable plaintext*—message is very likely to have certain content, such as a date header
  - *Chosen plaintext*—the attacker gains sufficient access to the system to generate ciphertext from arbitrary plaintext inputs

Cryptographic Primitives

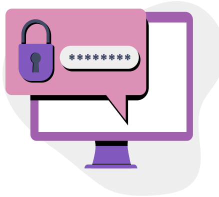


Substitution

One set of bits is exchanged for another

Transposition

Rearranging the order of the ciphertext to break any repeating patterns in the underlying plaintext



Confusion

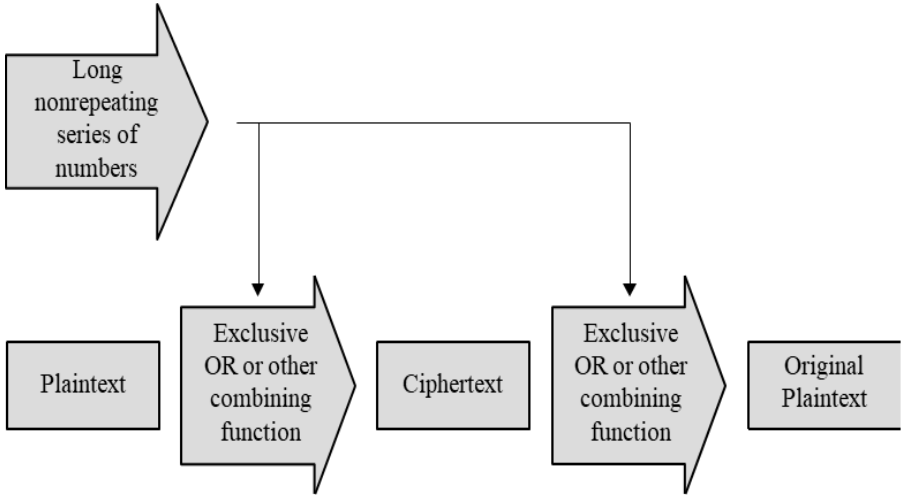
An algorithm providing good confusion has a complex functional relationship between the plaintext/key pair and the ciphertext, so that changing one character in the plaintext causes unpredictable changes to the resulting ciphertext.

Diffusion

Distributes the information from single plaintext characters over the entire ciphertext output, so that even small changes to the plaintext result in broad changes to the ciphertext

One-Time Pads

- A substitution cipher
- Uses an arbitrarily large, nonrepeating set of keys
  - (E.g. Vernam cipher)
- Offers no patterns to analyze
- Useful as a concept but completely impractical




```
      H      E      L      L      O   message
    7 (H)  4 (E) 11 (L) 11 (L) 14 (O) message
+  23 (X) 12 (M)  2 (C) 10 (K) 11 (L) key
=  30     16     13     21     25     message + key
=   4 (E) 16 (Q) 13 (N) 21 (V) 25 (Z) message + key (mod 26)
      E      Q      N      V      Z   → ciphertext
```

```
      E      Q      N      V      Z   ciphertext
    4 (E) 16 (Q) 13 (N) 21 (V) 25 (Z) ciphertext
-  23 (X) 12 (M)  2 (C) 10 (K) 11 (L) key
= -19      4     11     11     14     ciphertext - key
=   7 (H)  4 (E) 11 (L) 11 (L) 14 (O) ciphertext - key (mod 26)
      H      E      L      L      O   → message
```

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	12	22	23	24	25

Making "Good" Encryption Algorithms

What Makes a "Secure" Encryption Algorithm?

What does it mean for a cipher to be "good"?

- **The meaning of good depends on the intended use of the cipher**
  - A cipher to be used by military personnel in the field has different requirements from one to be used in a secure installation with substantial computer support

Shannon's Characteristics of "Good" Ciphers

1. **The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.**

Shannon's Characteristics of "Good" Ciphers

2. **The set of keys and the enciphering algorithm should be free from complexity**

- ✓ If the process is too complex, it will not be used
- ✓ Choice of keys & the types of plaintext should not be restricted
  - An algorithm that works only on plaintext having an equal number of A's and E's is useless
  - Requiring the key to be a prime number is challenging
- ✓ Furthermore, the key must be transmitted, stored, and remembered so it must be short..

Shannon's Characteristics of "Good" Ciphers

3. **The implementation of the process should be as simple as possible**
   - ✓ A complicated algorithm is prone to error or likely to be forgotten
   - ✓ People tend to avoid an encryption algorithm if its implementation process severely hinders message transmission
   - ✓ Not to mention, a complex algorithm is more likely to be programmed incorrectly.

Shannon's Characteristics of "Good" Ciphers

4. **The size of the enciphered text should be no larger than the text of the original message**
   - ✓ ciphertext that expands dramatically in size cannot possibly carry more information than the plaintext
   - ✓ it gives the cryptanalyst more data from which to infer a pattern
   - ✓ longer ciphertext implies more space for storage and more time to communicate

Shannon's Characteristics of "Good" Ciphers

5. **Errors in ciphering should not propagate and cause corruption of further information in the message**
   - One error early in the process should not throw off the entire remaining ciphertext
   - For example, dropping one letter in a columnar transposition throws off the entire remaining encipherment

Those characteristics have been proposed in 1949, Do you think it is still valid?

Properties of a Trustworthy Cryptosystem

An encryption system is "commercial grade," or "trustworthy," we mean that it meets these constraints

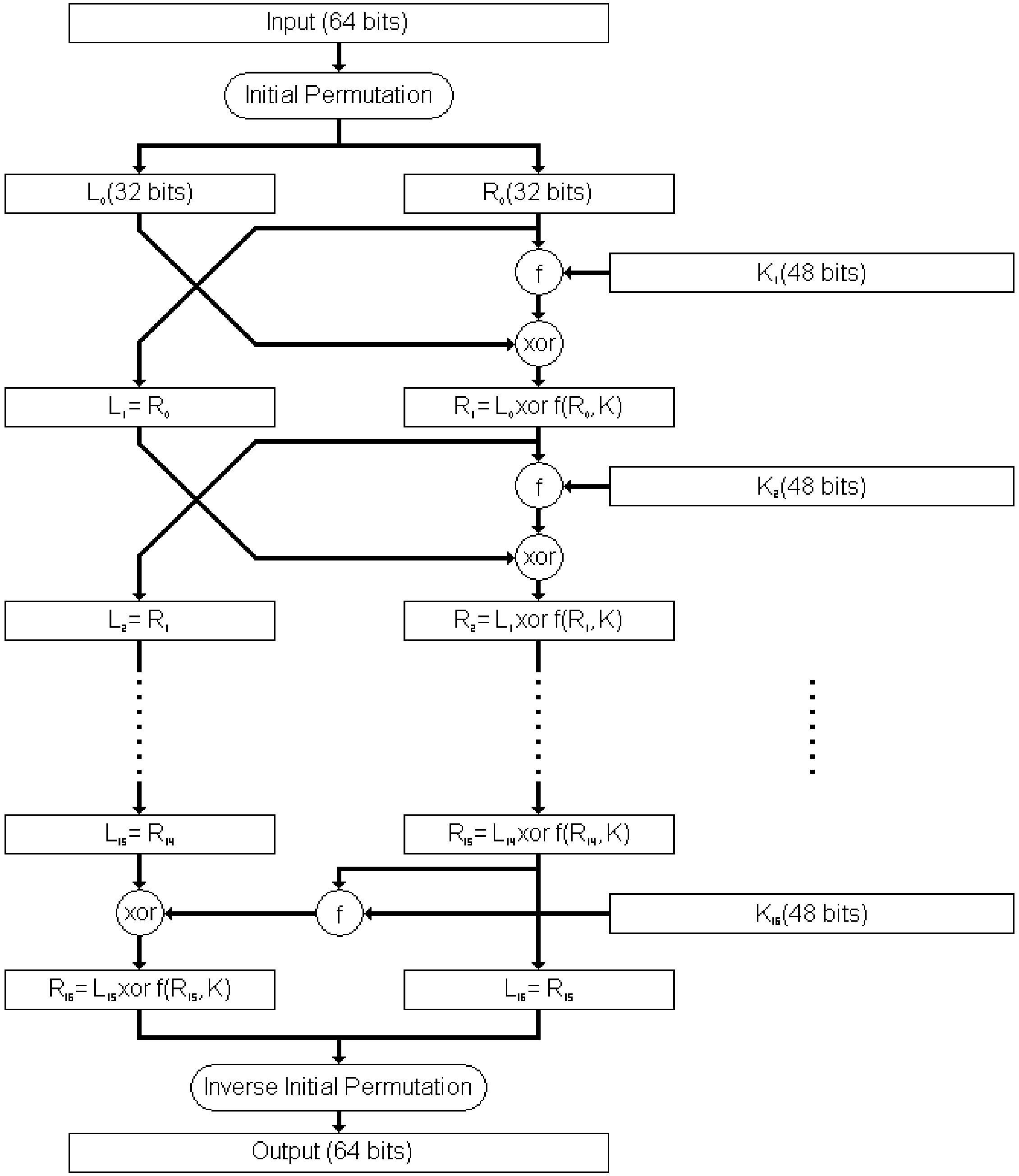
- It is based on sound mathematics.
- It has been analyzed by competent experts and found to be sound.
- It has stood the test of time

Three algorithms are popular in the commercial world and meet the above criteria:

- DES (data encryption standard)
- AES (advanced encryption standard)
- RSA (Rivest Shamir Adelman)

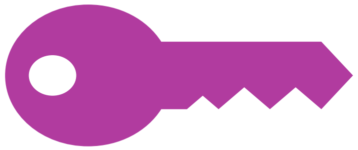
DES

The Data Encryption Standard



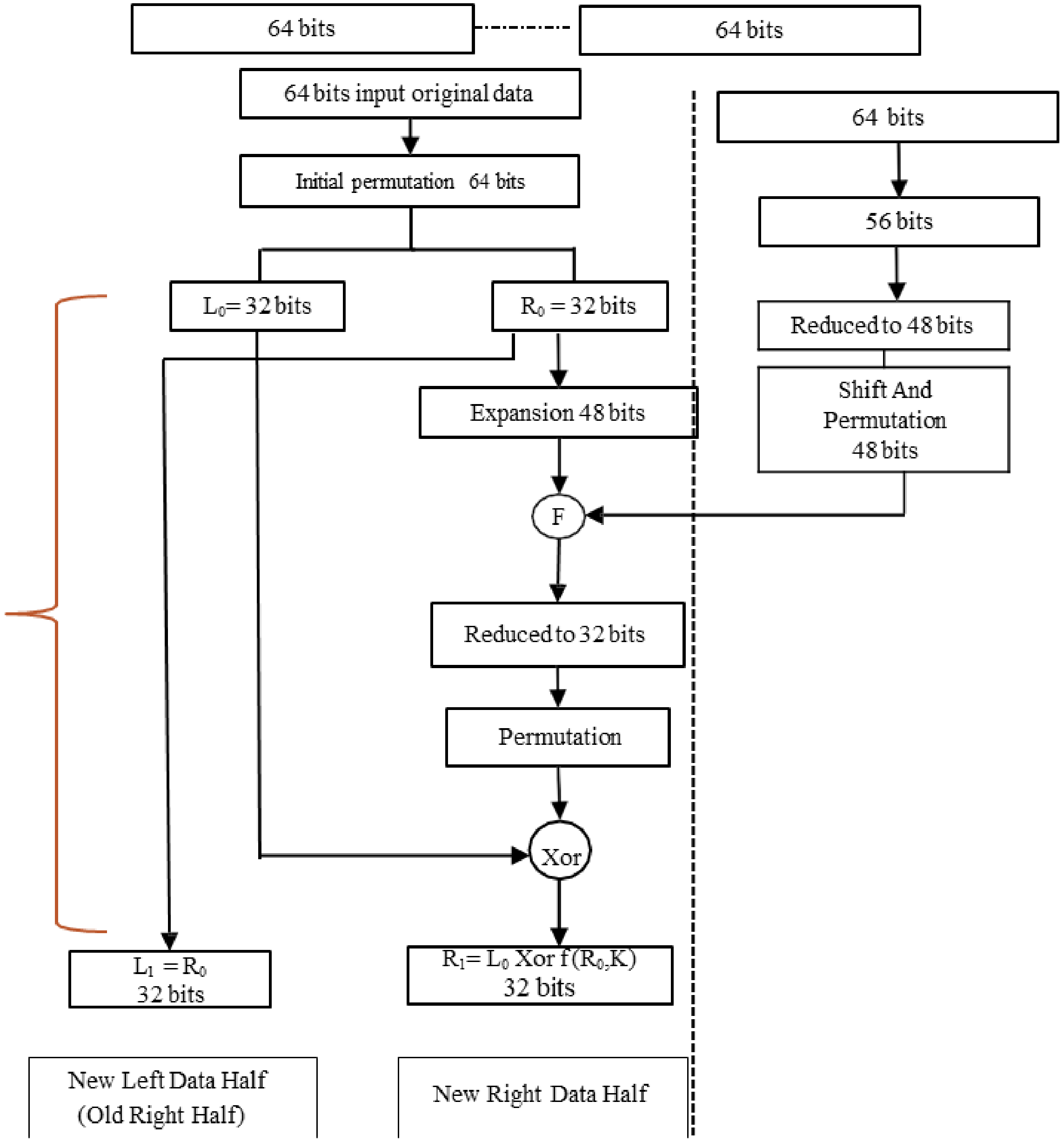
DES

- ✓ Developed for the U.S. government in 1976
- ✓ Intended for use by general public.
- ✓ Accepted as a standard both in the US and abroad.
- ✓ Many hw and sw systems have been designed to accommodate the DES
- ✓ However, recently its adequacy has been questioned.



2 stages: key preparation and message encryption

- ✓ Input message is divided into blocks of 64 bits
- ✓ The data bits are permuted by an "initial permutation"
- ✓ The 64 permuted data bits are broken into a left half and right half
- ✓ The 32-bit right half is expanded to 48 bits by repeating certain bits
- ✓ The key is reduced from 64 bits to 56 bits (parity bits are removed)
- ✓ The key is reduced to 48 bits by choosing only certain bits
  - ✓ according to tables called S-boxes
- ✓ The key is shifted left by a number of bits and also permuted
- ✓ **The key is combined with the right half, which is then combined with the left half**
- ✓ **The result of these combinations becomes the new right half, while the old right half becomes the new left half.**



DES Decryption Equation

$$L_j = R_{j-1} \quad (1)$$

$$R_j = L_{j-1} \oplus f(R_{j-1}, k_j) \quad (2)$$

By rewriting these equations in terms of R_{j-1} and L_{j-1}, we get

$$R_{j-1} = L_j \quad (3)$$

and

$$L_{j-1} = R_j \oplus f(R_{j-1}, k_j) \quad (4)$$

Substituting (3) into (4) gives

$$L_{j-1} = R_j \oplus f(L_j, k_j) \quad (5)$$

DES

https://www.youtube.com/watch?time_continue=1&v=uqZivwCDfik&feature=emb_logo

DES Weakness

Suppose… Zelda can see the ciphertext form and she knows where to look for the different fields.

What can she do?

64 bits

	Date	From acct	To acct	Trf Num	Amount
	1 Aug	Annie	Brian	0001	100.00
ciphertext	apqrwx	w2z%pr	grd#d#	wenh55	3dhop3
	1 Aug	Carole	Drew	0002	500.00
	apqrwx	df7ynm	gyl615	23opdw	kslw4l
	1 Aug	Evin	Zelda	0003	0.01
	apqrwx	bze4n4	cd4wx7	wenh55	otm4m5
	1 Aug	Feng	Zelda	0004	0.01
	apqrwx	br5hun	cd4wx7	ztpztp	otm4m5

Fabricated Transfer Messages (Possible Attack)

she can create new messages, to transfer money from Annie and Carole to her account

1 Aug	Annie	Zelda	0001	100.00
apqrwx	w2z%pr	cd4wx7	wenh55	3dhop3

1 Aug	Carole	Zelda	0002	500.00
apqrwx	df7ynm	cd4wx7	ztpztp	kslw4l

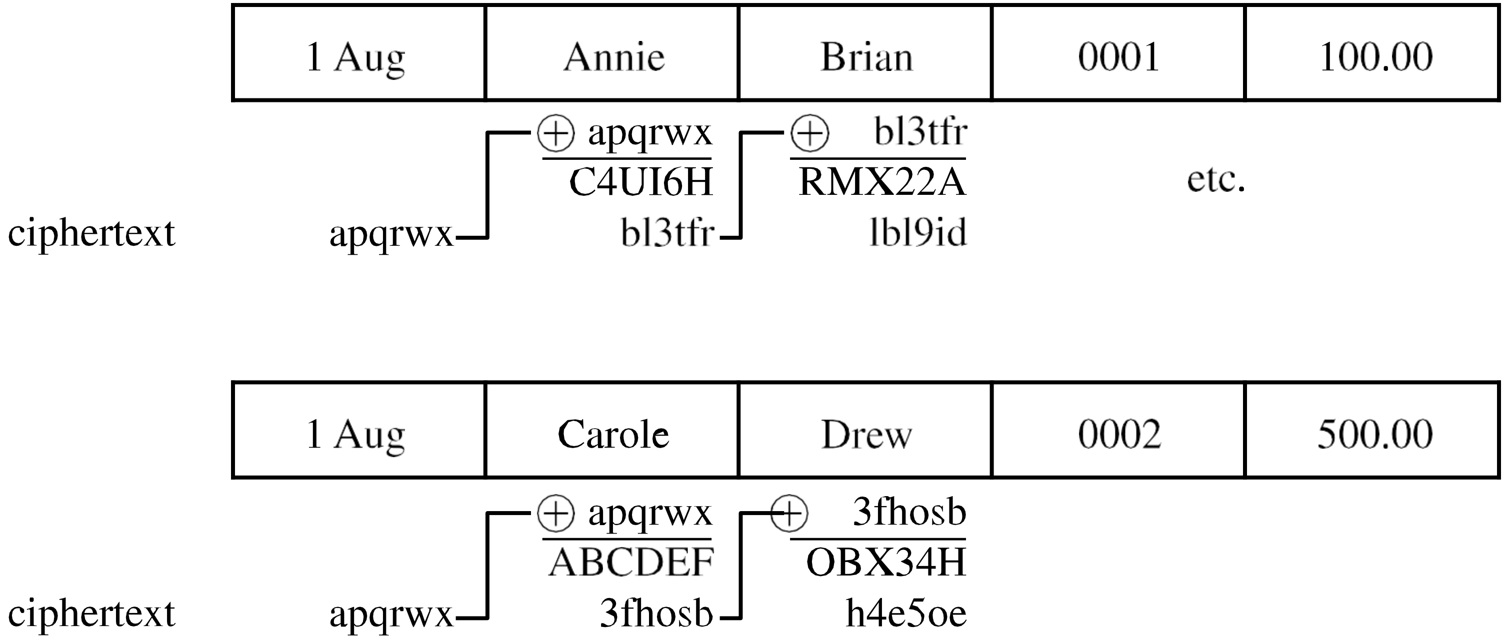
Chaining

DES uses the same process for each 64-bit block, so two identical blocks encrypted with the same key will have identical output

This provides too much information to an attacker, as messages that have common beginnings or endings, for example, are very common in real life, as is reuse of a single key over a series of transactions

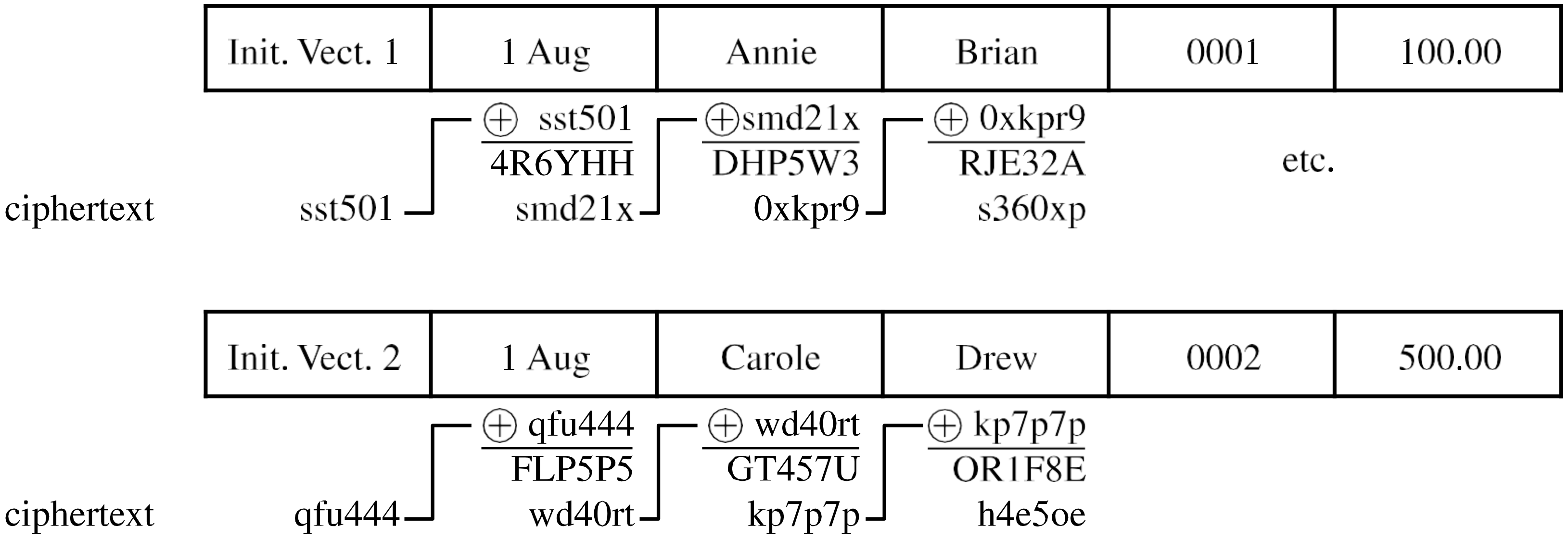
The solution to this problem is **chaining**, which makes the encryption of each block dependent on the content of the previous block as well as its own content

Simple Chaining Example



Still there is a problem!!!

Initialization Vectors



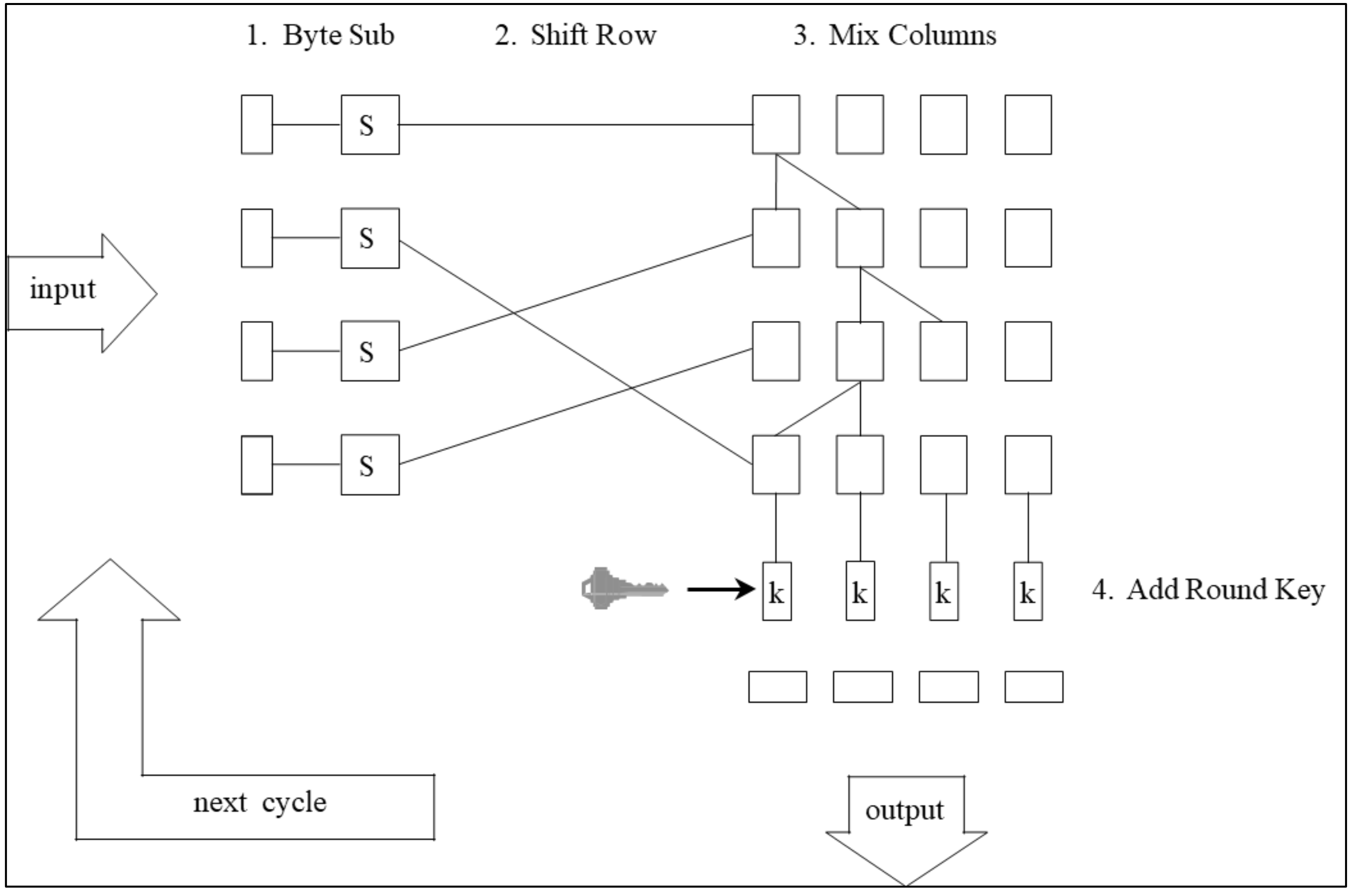
AES

Advanced Encryption System

Because of the concerns about the fixed-sized key of DES and the fact that computing power was continually increasing against that stationary target, security analysts began to search for a replacement for DES

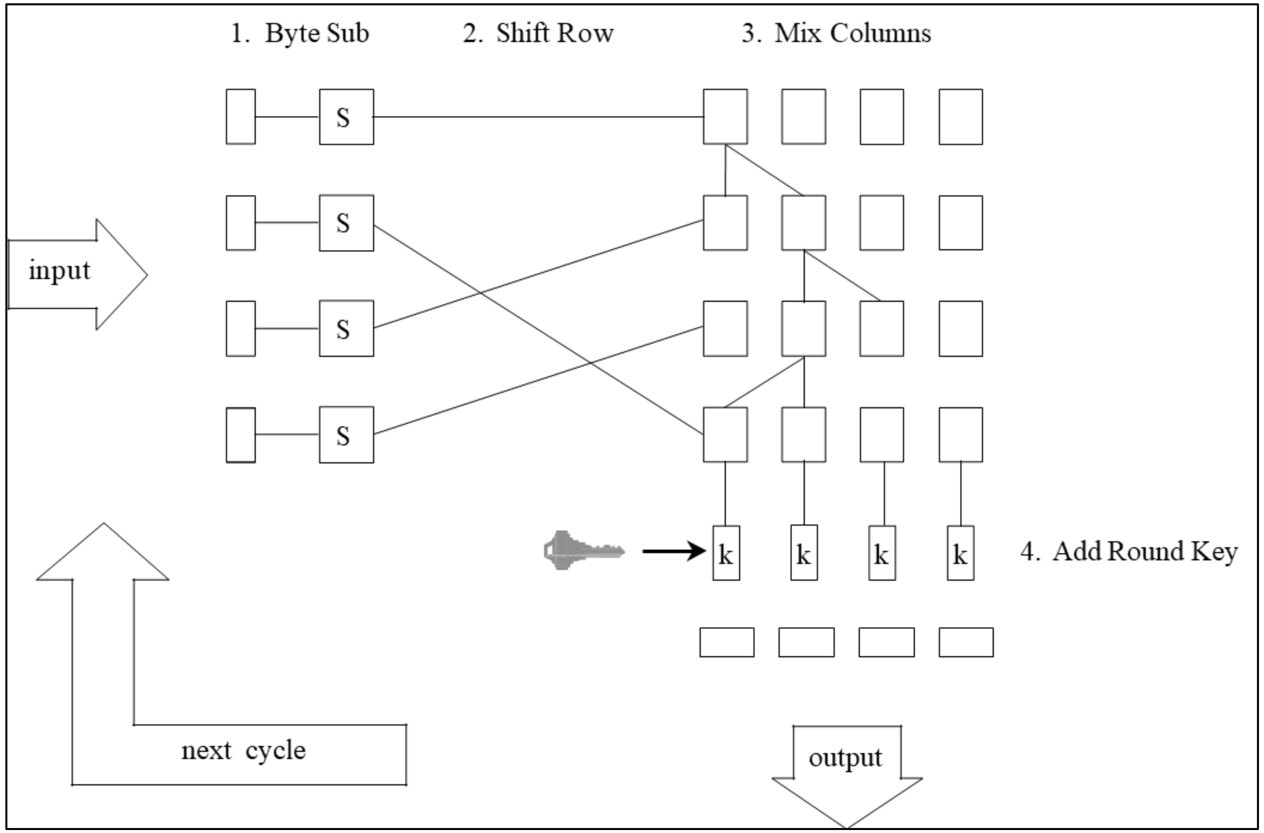
Structure of AES

The algorithm is based on arithmetic in the finite field GF(2 8), but most encryption operations can be done by table lookup, thereby simplifying the implementation of AES.



- ✓ The block size of AES is 128.
- ✓ AES consists of 10, 12 or 14 cycles, for a 128-, 192-, or 256-bit key, respectively.
- ✓ Each cycle (called a “round” in the algorithm).
- ✓ Steps for AES:
  - Convert to state array
  - Transformations (and their inverses)
    - AddRoundKey
    - SubBytes
    - ShiftRows
    - MixColumns
  - Key Expansion

Structure of AES

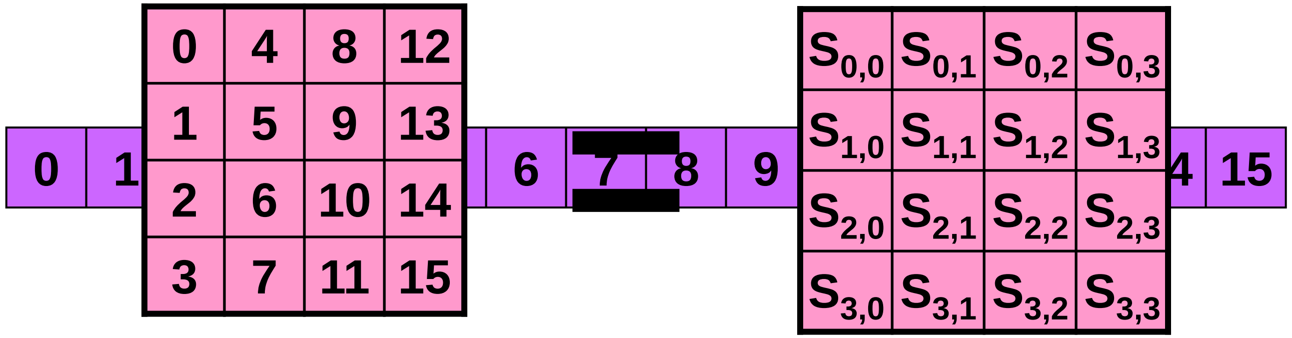


3 Phases

- Phase 1
  Initial Phase
  - Add round key
- Phase 2
  Main rounds
  - Sub Bytes
  - Shift Rows
  - Mix Columns
  - Add Round Key
- Phase 3
  Final Round
  - Sub Bytes
  - Shift Rows
  - Add Round Key

Convert to State Array

Input block:



Convert to State Array

Eg. Plain Text : AES USES A MATRIX ZZ

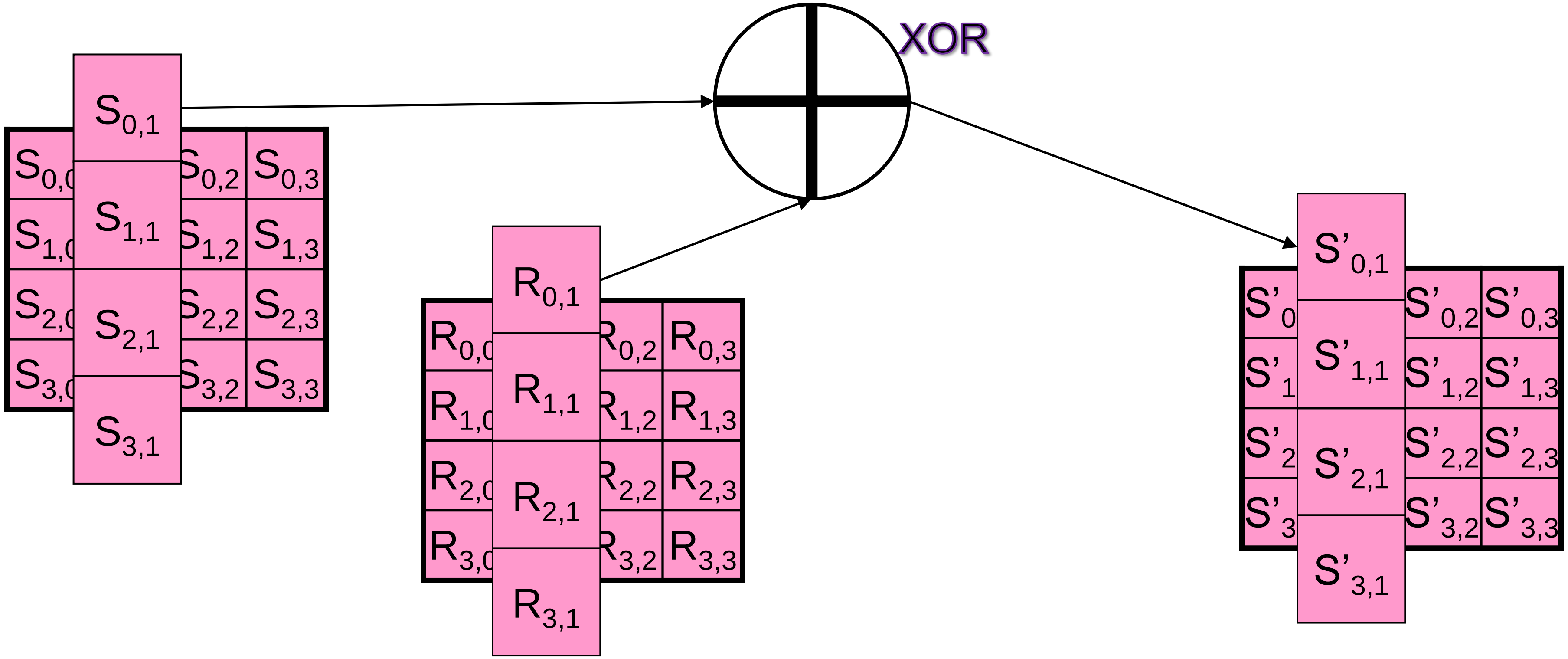
Hexadecimal : 00 04 12 14 12 04 12 00 0C 00 13 11 08 23 19 19

State			
00	12	0C	08
04	04	00	23
12	12	13	19
14	00	11	19

State representation

AddRoundKey

XOR each byte of the round key with its corresponding byte in the state array



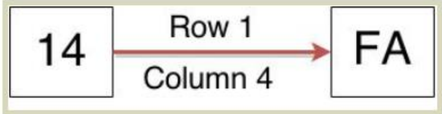
SubBytes

- Replace each byte in the state array with its corresponding value from the S-Box

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

SubBytes

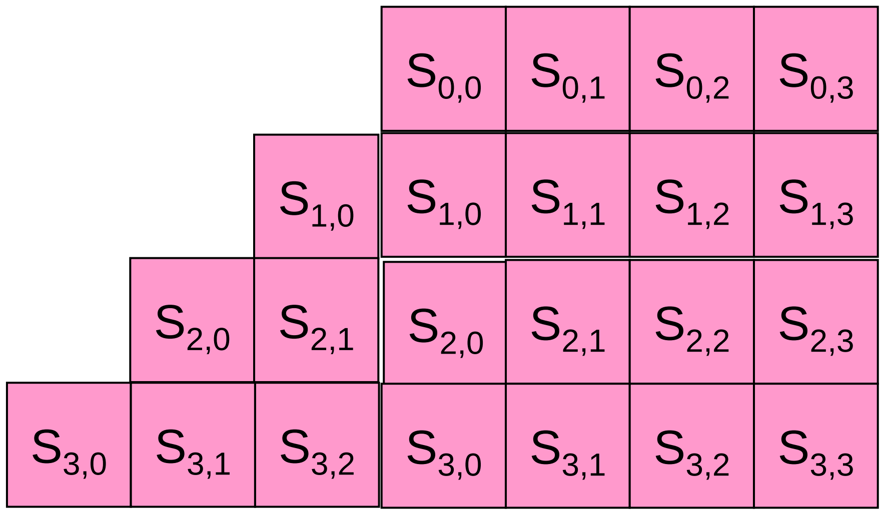
State			
00	12	0C	08
04	04	00	23
12	12	13	19
14	00	11	19



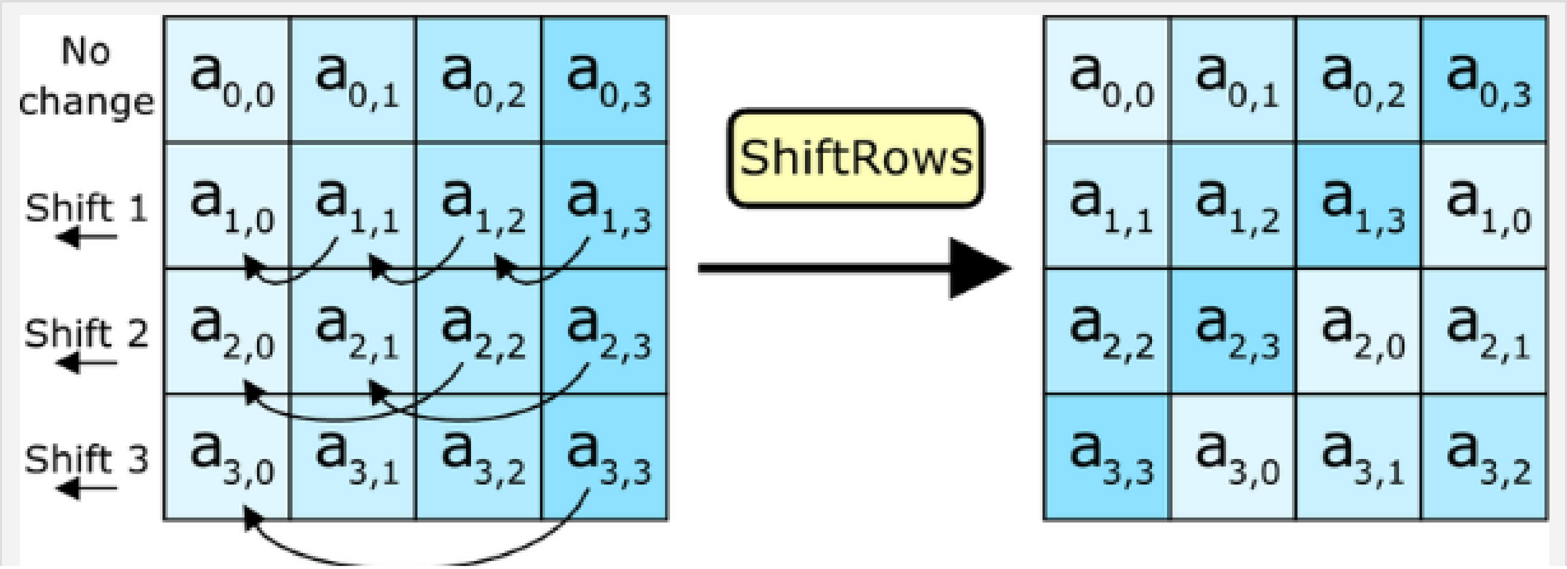
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

ShiftRows

- ✓ Last three rows are cyclically shifted

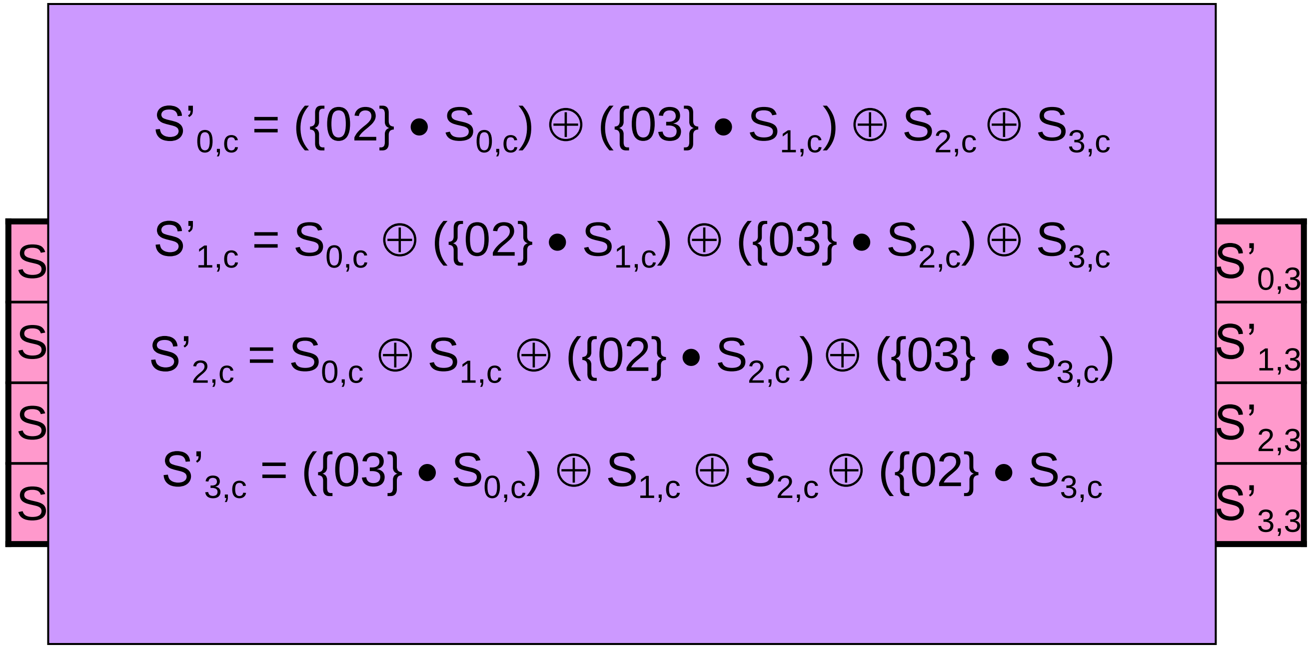


ShiftRows



MixColumns

- ✓ Apply MixColumn transformation to each column



$$S'_{0,c} = (\{02\} \bullet S_{0,c}) \oplus (\{03\} \bullet S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$$

$$S'_{1,c} = S_{0,c} \oplus (\{02\} \bullet S_{1,c}) \oplus (\{03\} \bullet S_{2,c}) \oplus S_{3,c}$$

$$S'_{2,c} = S_{0,c} \oplus S_{1,c} \oplus (\{02\} \bullet S_{2,c}) \oplus (\{03\} \bullet S_{3,c})$$

$$S'_{3,c} = (\{03\} \bullet S_{0,c}) \oplus S_{1,c} \oplus S_{2,c} \oplus (\{02\} \bullet S_{3,c}$$

MixColumns

$$\begin{bmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{bmatrix}$$

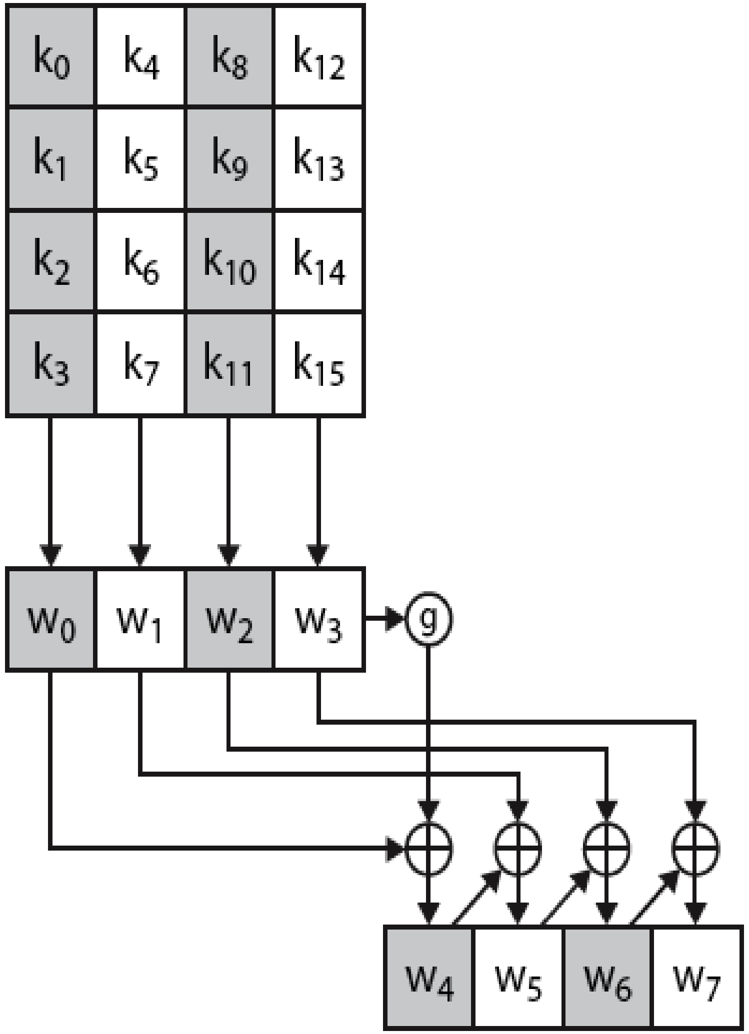
$$S'_{0,c} = (\{02\} \bullet S_{0,c}) \oplus (\{03\} \bullet S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$$

$$S'_{1,c} = S_{0,c} \oplus (\{02\} \bullet S_{1,c}) \oplus (\{03\} \bullet S_{2,c}) \oplus S_{3,c}$$

$$S'_{2,c} = S_{0,c} \oplus S_{1,c} \oplus (\{02\} \bullet S_{2,c}) \oplus (\{03\} \bullet S_{3,c})$$

$$S'_{3,c} = (\{03\} \bullet S_{0,c}) \oplus S_{1,c} \oplus S_{2,c} \oplus (\{02\} \bullet S_{3,c})$$

Key Expansion

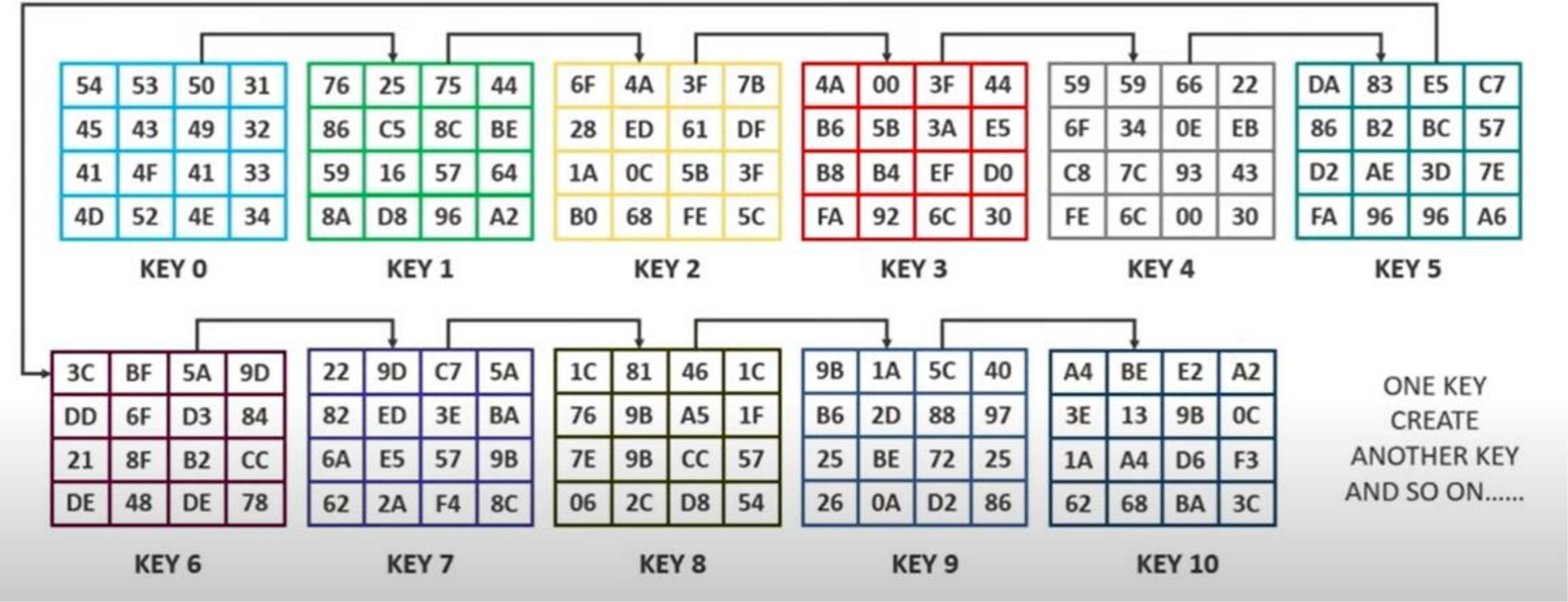


- ✓ Expands the key material so that each round uses a unique round key
  - Generates Nb(Nr+1) words
    - Nb is the number of words in an AES block
    - Nr is the number of rounds

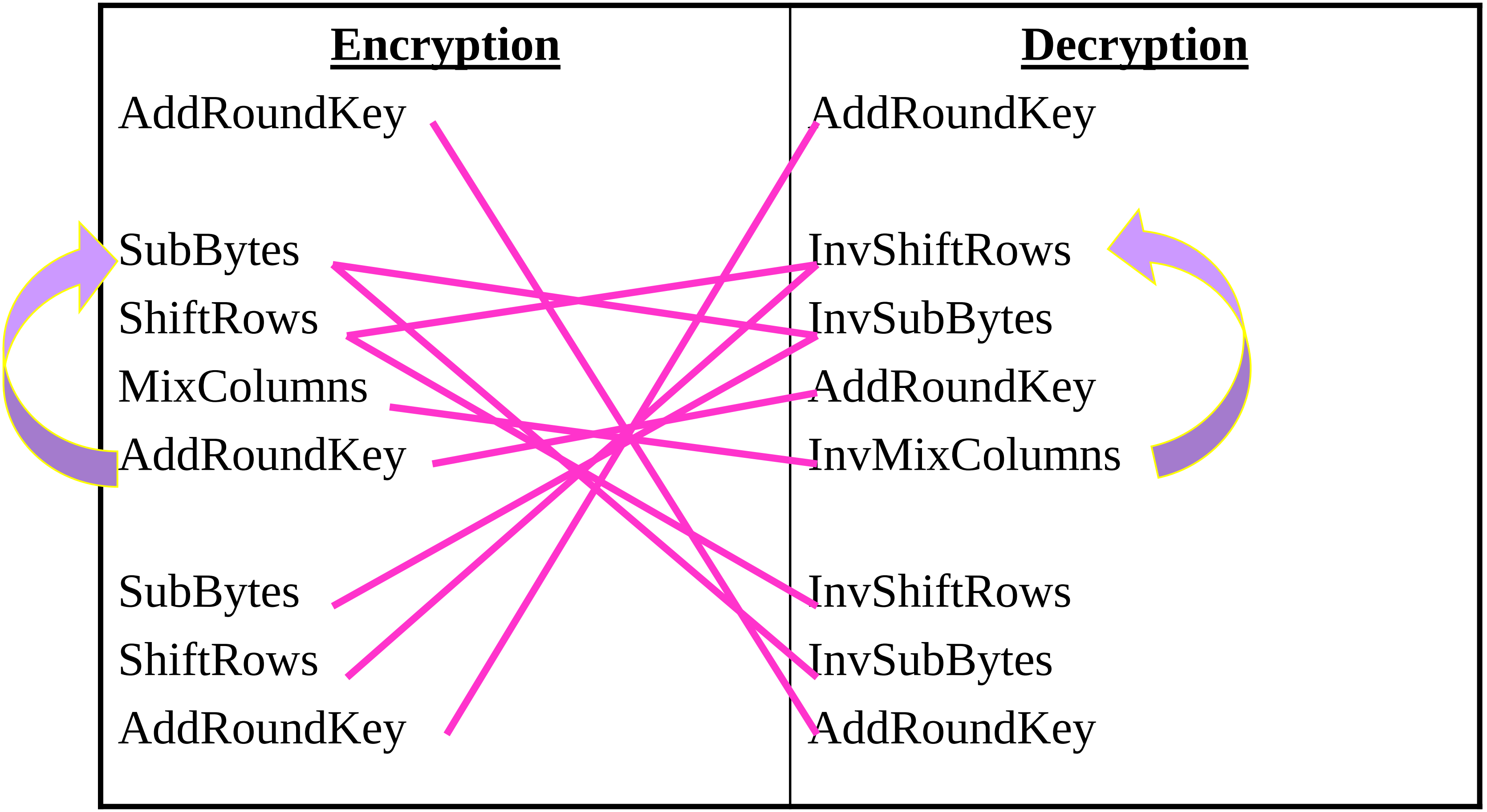
Word: **A group of 32 bits that is treated either as a single entity or as an array of 4 bytes**

Expanded Key Sizes in Words		
Key Length *(Nk words)*	**Number of Rounds** *(Nr)*	**Exp. Key Size** *(Nb(Nr+1) words)*
4	10	44
6	12	52
8	14	60

Key Expansion



Encrypt and Decrypt



Longevity of AES

- ✓ Since its initial publication in 1997, AES has been extensively analyzed, and the only serious challenges to its security have been highly specialized.
- ✓ Because there is an evident underlying structure to AES, it will be possible to use the same general approach on a slightly different underlying problem to accommodate keys larger than 256 bits when necessary
- ✓ No attack to date has raised serious question as to the overall strength of AES

RSA

Rivest Shamir Adelman

RSA

- ✓ **Asymmetric Encryption**
- ✓ **RSA has been the subject of extensive cryptanalysis since 1978**
  - no serious flaws have yet been found
- ✓ **The encryption algorithm is based on the underlying problem of factoring large prime numbers**
  - a problem for which the fastest known algorithm is exponential in time
- ✓ **Two keys, *d* and *e*, are used for decryption and encryption (they are interchangeable)**
  - The plaintext block P is encrypted as $P^e \bmod n$
  - The decrypting key d is chosen so that $(P^e)^d \bmod n = P$

Detailed Description of RSA

The RSA algorithm uses two keys, d and e, which work in pairs, for decryption and encryption, respectively. A plaintext message P is encrypted to ciphertext C by

$$C = P^e \bmod n$$

The plaintext is recovered by

$$P = C^d \bmod n$$

Because of symmetry in modular arithmetic, encryption and decryption are mutual inverses and commutative. Therefore,

$$P = C^d \bmod n = (P^e)^d \bmod n = (P^d)^e \bmod n$$

This relationship means that one can apply the encrypting transformation and then the decrypting one, or the decrypting one followed by the encrypting one.

Prime and Coprime numbers

- ✓ **Prime numbers** are divisible only by the **number** 1 or itself.
- ✓ For example, 2, 3, 5, 7 and 11 are the first few **prime numbers**.
- ✓ Two integers ***a*** and ***b*** are said to be ***relatively prime,*** if the only positive integer (factor) that divides both of them is 1

Deriving an RSA Key Pair

1. The encryption key consists of the pair of integers (e, n), and the decryption key is (d, n)
2. The value of n should be quite large, a product of two primes, p and q
   - Typically, p and q are nearly 100 digits each, so n is approximately 200 decimal digits (about 512 bits) long.
   - A large value of n effectively inhibits factoring n to infer p and q (but time to encrypt increases as the value of n grows larger)
3. A relatively large integer e is chosen so that e is relatively prime to $(p - 1) * (q - 1)$. An easy way to guarantee that e is relatively prime to $(p - 1) * (q - 1)$ is to choose e as a prime that is larger than both $(p - 1)$ and $(q - 1)$
4. Finally, select d such that $e * d = 1 \mod (p - 1) * (q - 1)$
5. Due to increased computing power, 2048-bit keys are becoming a standard requirement

RSA

A very simple example of RSA encryption

1. Select primes **p=11, q=3**
2. Compute **n = p*q = 11 * 3 = 33**
3. Compute (p-1)*(q-1) = 10 * 2 = 20
4. Choose e=3, 1<3<20
5. Check gcd(e, (p-1 * q-1)) = gcd(3, 20) = 1

   (i.e. 3 and 20 have no common factors except 1).
6. Compute d such that e*d ≡ 1 (mod (p-1)(q-1))

   i.e. compute 3 * d = 1 mod 20. We get d=7
7. Public key = (e,n) = (3,33)

   Private key = (d,n) = (7,33).

The greatest common divisor (gcd): gcd of two numbers is the largest number that divides them both.

Message Digests

- **Message digests are ways to detect changes to a block of data**
- **One-way hash functions are cryptographic functions with multiple uses:**
  - They are used in conjunction with public-key algorithms for both encryption and digital signatures
  - They are used in integrity checking
  - They are used in authentication
  - They are used in communications protocols
- **Modern hash functions meet two criteria:**
  - They are **one-way**, meaning they convert input to a digest, but it is infeasible to start with a digest value and infer the input
  - They do **not** have **obvious collisions**, meaning that it is infeasible to find a pair of inputs that produce the same digest

Properties of Current Hash Standards

Algorithm	Maximum Message Size (bits)	Block Size (bits)	Rounds	Message Digest Size (bits)
MD5	2^{64}	512	64	128
SHA-1	2^{64}	512	80	160
SHA-2-224	2^{64}	512	64	224
SHA-2-256	2^{64}	512	64	256
SHA-2-384	2^{128}	1024	80	384
SHA-2-512	2^{128}	1024	80	512
SHA-3-256	unlimited	1088	24	256
SHA-3-512	unlimited	576	24	512

Digital Signatures

Digital signatures must meet two requirements and, ideally, satisfy two more:

Unforgeable (mandatory)

No one other than the signer can produce the signature without the signer's private key

Authentic (mandatory)

The receiver can determine that the signature really came from the signer

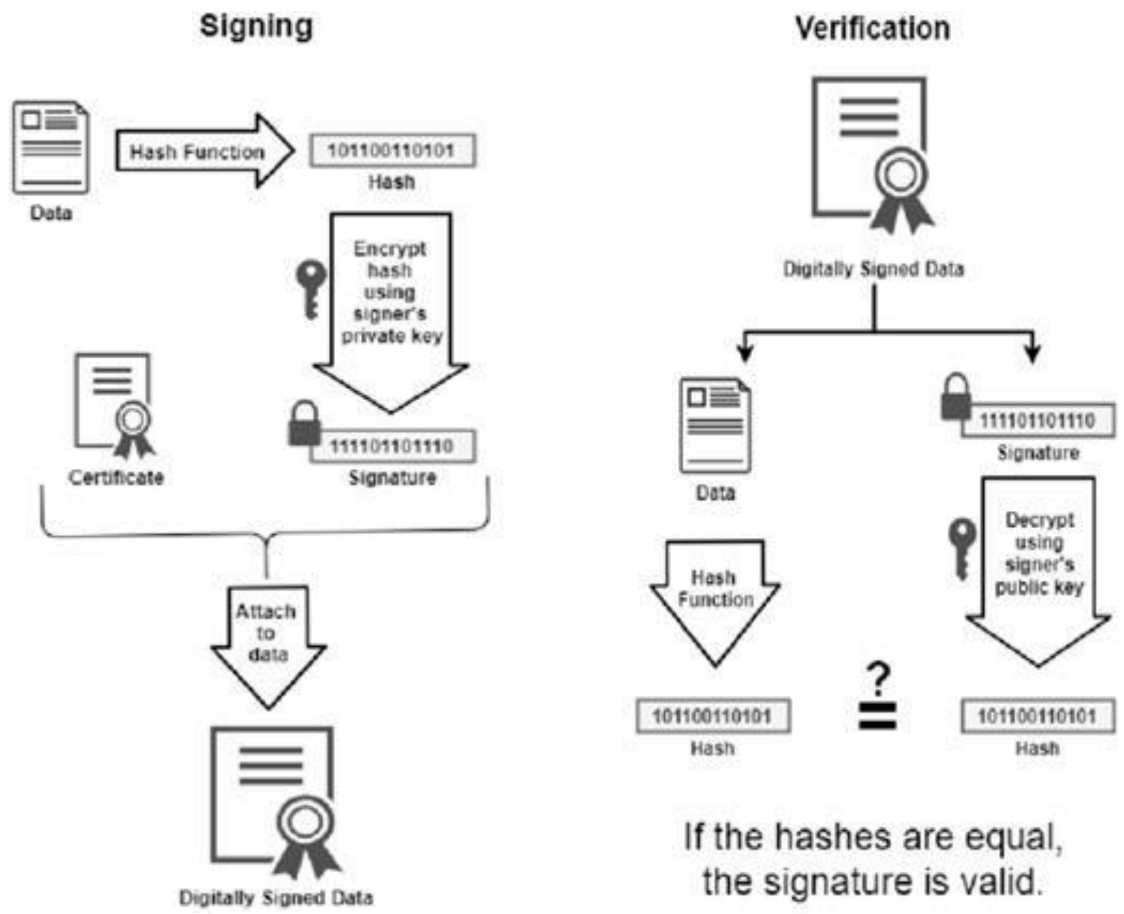
Not alterable (desirable)

No signer, receiver, or any interceptor can modify the signature without the tampering being evident

Not reusable (desirable)

Any attempt to reuse a previous signature will be detected by receiver

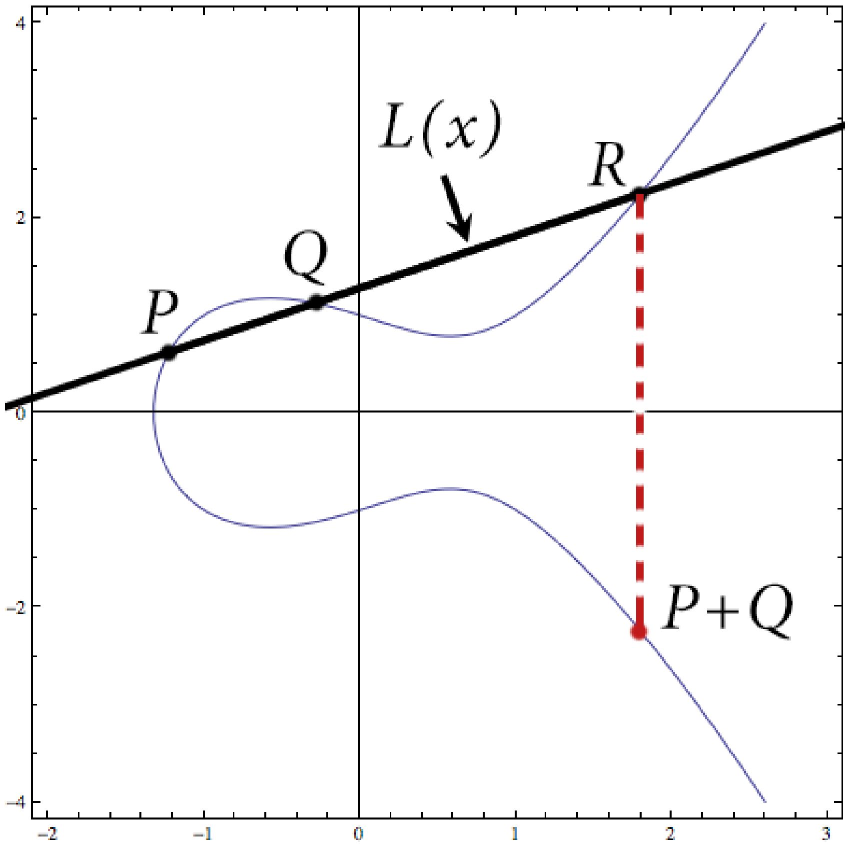
Digital Signatures



The general way of computing digital signatures is with public key encryption:

- The signer computes a signature value by using a private key.
- Others can use the public key to verify that the signature came from the corresponding private key

Elliptic Curve Cryptosystems



- ✓ While the RSA algorithm appears sufficiently strong, it has a different kind of flaw: *It is patented*
- ✓ An alternative form of asymmetric cryptography comes in the form of Elliptic Curve Cryptography (ECC)
- ✓ ECC has two advantages over RSA:
  - While some technologies using ECC are patented, the general algorithm is in the public domain.
  - ECC can provide similar security to RSA using a shorter key length.

Quantum Cryptography

- ✓ Based on physics, not mathematics- using light particles called *photons*.
- ✓ It relies on ability to measure certain properties of photons and on Heisenberg's uncertainty principle
    - allows senders and receivers in quantum communication to easily detect eavesdroppers
- ✓ Implementations still in the prototype stage
    - creating practical photon guns and receivers is technically difficult
- ✓ While still not ready for adoption, quantum cryptography may be practical within the next decade
    - would likely be a significant improvement over existing systems for encrypted communication

https://images.app.goo.gl/Cc4BX2Q5zCwHHG599

Summary

- Substitution, transposition, confusion, and diffusion are the basic primitives of cryptography
- DES is a relatively simple symmetric algorithm that, although no longer practical, is useful for studying technique
- Chaining and random initialization vectors are important techniques for preventing ciphertext repetition
- AES remains the modern standard for symmetric encryption almost 20 years after its introduction
- RSA is a popular and deceptively simple algorithm for asymmetric cryptography
- Message digests use one- way cryptographic hash functions to detect message modification
- Digital signatures use asymmetric encryption to detect forged messages
- While not yet ready for mainstream use, quantum cryptography will likely be a significant improvement over modern encrypted communication

Extra Information

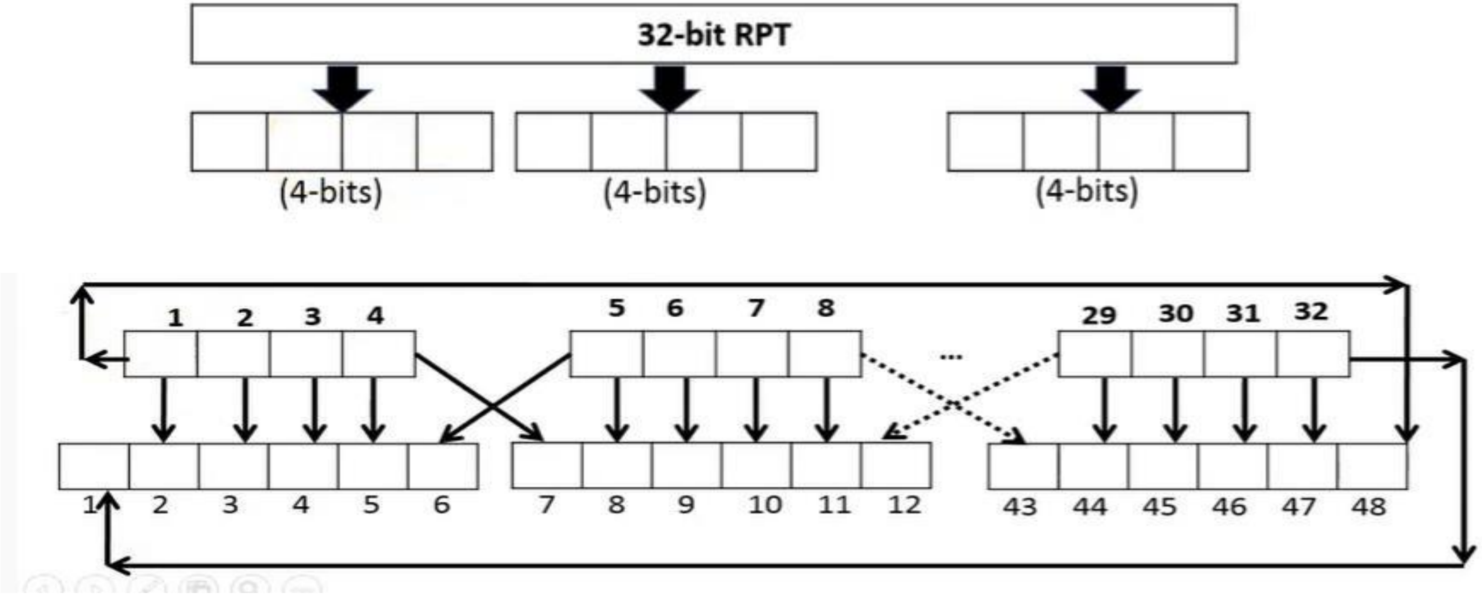
Initial permutation

- 1st bit take 40th position
- 58th bits take 1st position

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Expansion of 32 bits:

- 32 bit RH is divided into 8 blocks of 4 bits
- Expand each 4-bits block to 6-bits block

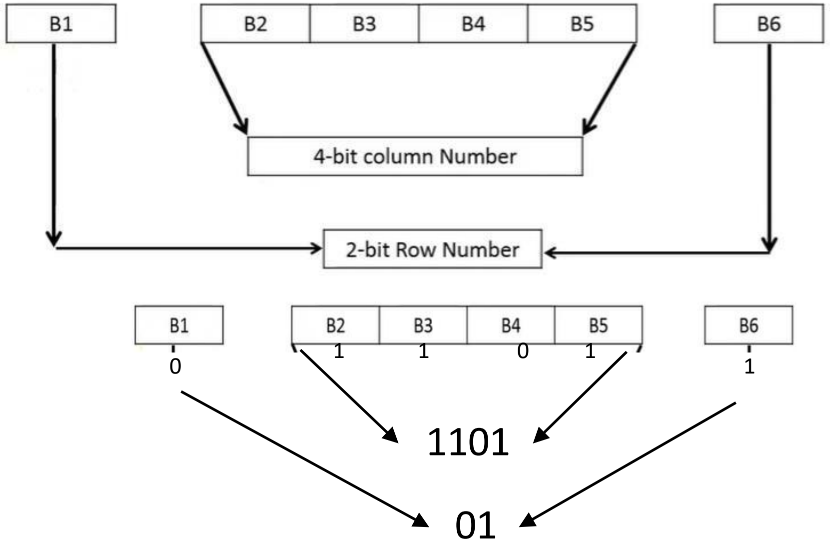


S-box

Example 011011

011011 → 01

1001



S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011