Hashes and Message Digests

- A **hash** or **message digest**, is a ***one-way function*** since it is not practical to reverse.
- A function is cryptographicaly secure if it is computationally infeasible to find:
  - a message that has a given message digest.
  - a different message with the same message digest.
  - two messages that have the same message digest.

Major Algorithms

- Ron Rivest ***Message Digest*** MD-family (***MD2, MD4*** and ***MD5***): 128-bit
- NIST ***Secure Hash Algorithm SHA-1***: 160-bit.
- They take an *arbitrary-length* string and map it to a *fixed-length* quantity that appears to be randomly chosen.
  For example, two inputs that differ by only one bit should have outputs that look like completely independently chosen random numbers.

Things to do with a Hash

- *Authentication*
- *Computing a MAC*
- *Encryption*
- *Using Secret Key for a Hash*

Authentication

- Requirements - must be able to verify that:
  1. Message came from apparent source or author,
  2. Contents have not been altered,
  3. Sometimes, it was sent at a certain time or sequence.

- Protection against active attack (falsification of data and transactions)

Approaches to Message Authentication

- Authentication Using Conventional Encryption
  - Only the sender and receiver should share a key
- Message Authentication without Message Encryption
  - An authentication tag is generated and appended to each message
- Message Authentication Code
  - Calculate the MAC as a function of the message and the key. MAC = F(K, M)

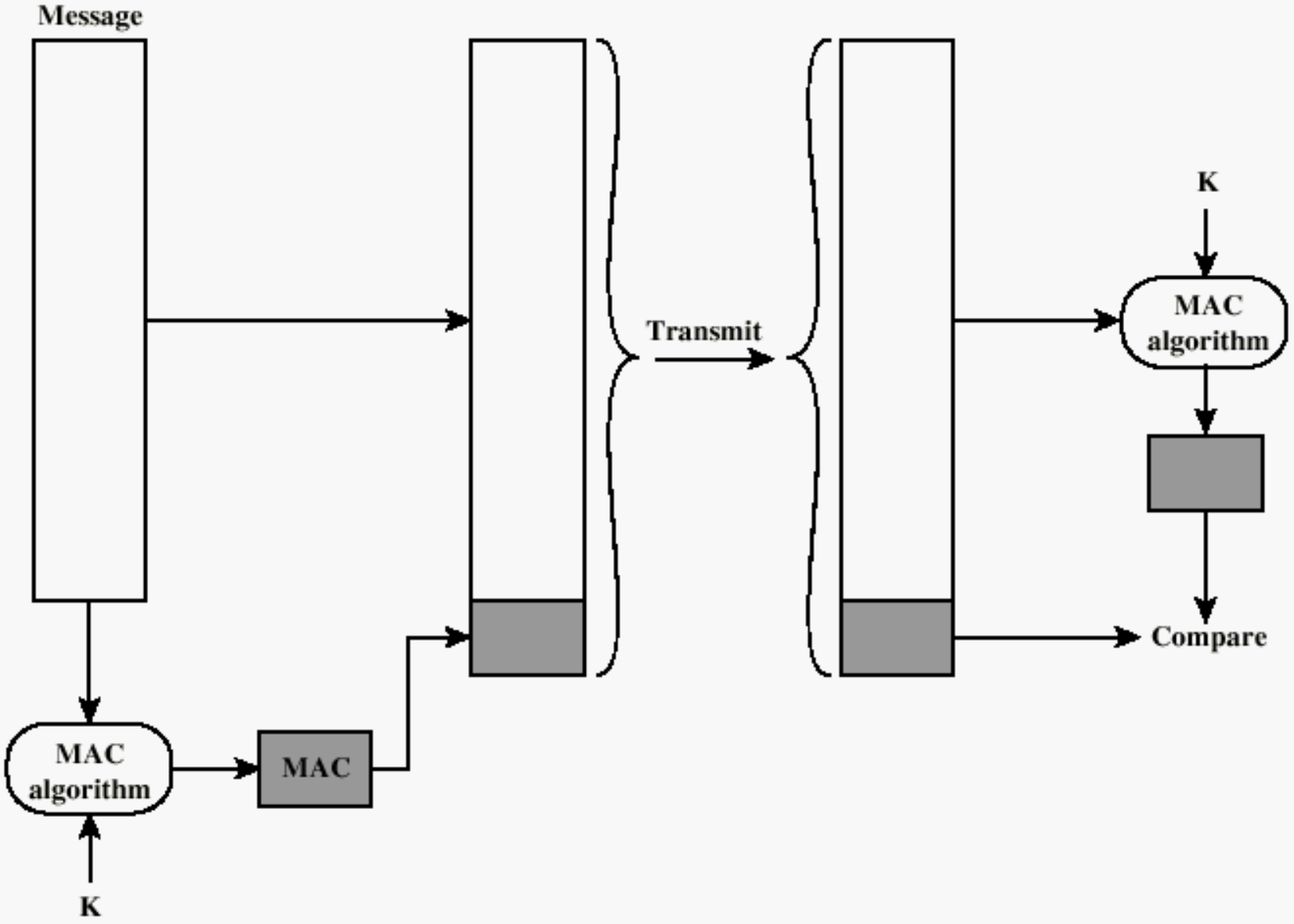
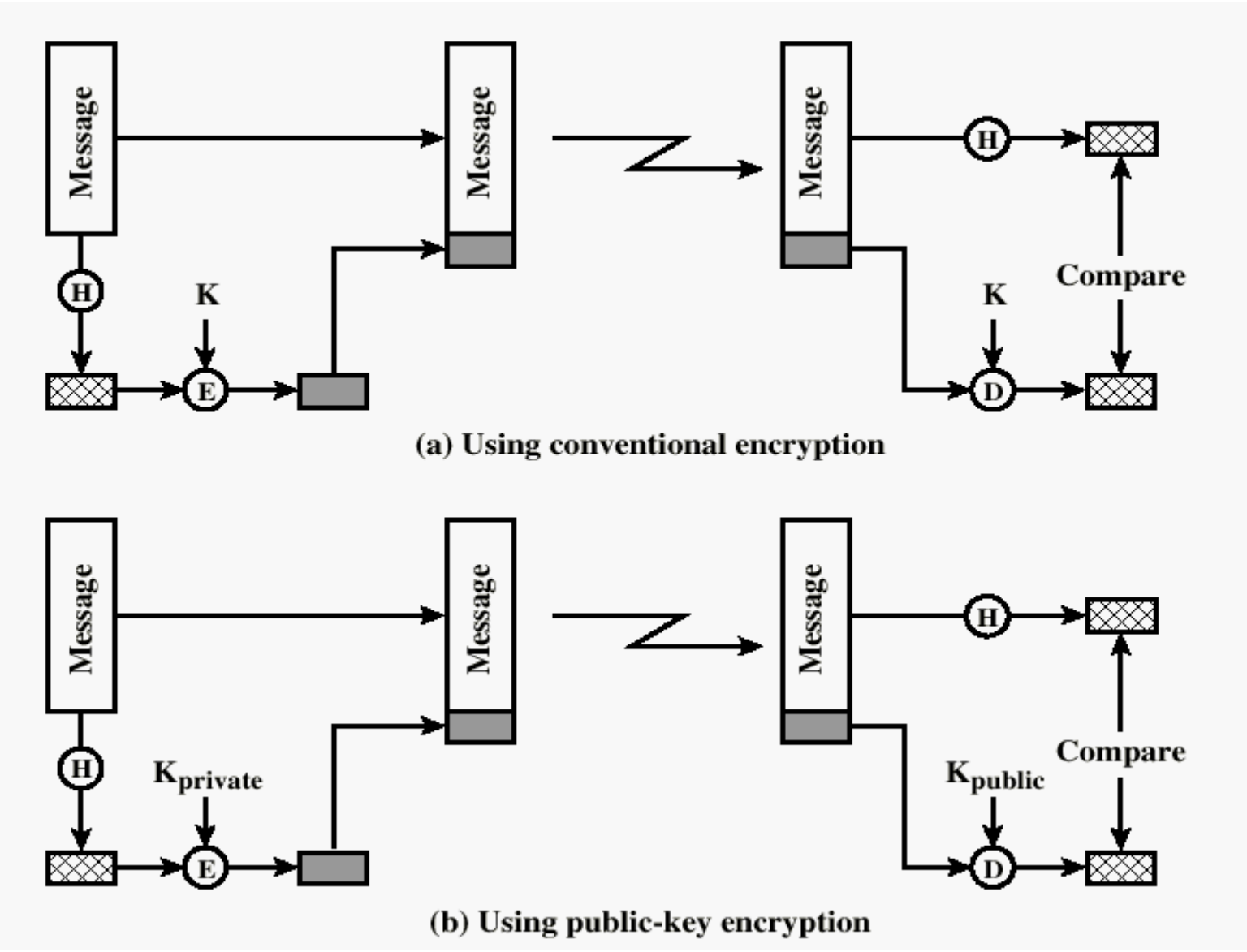


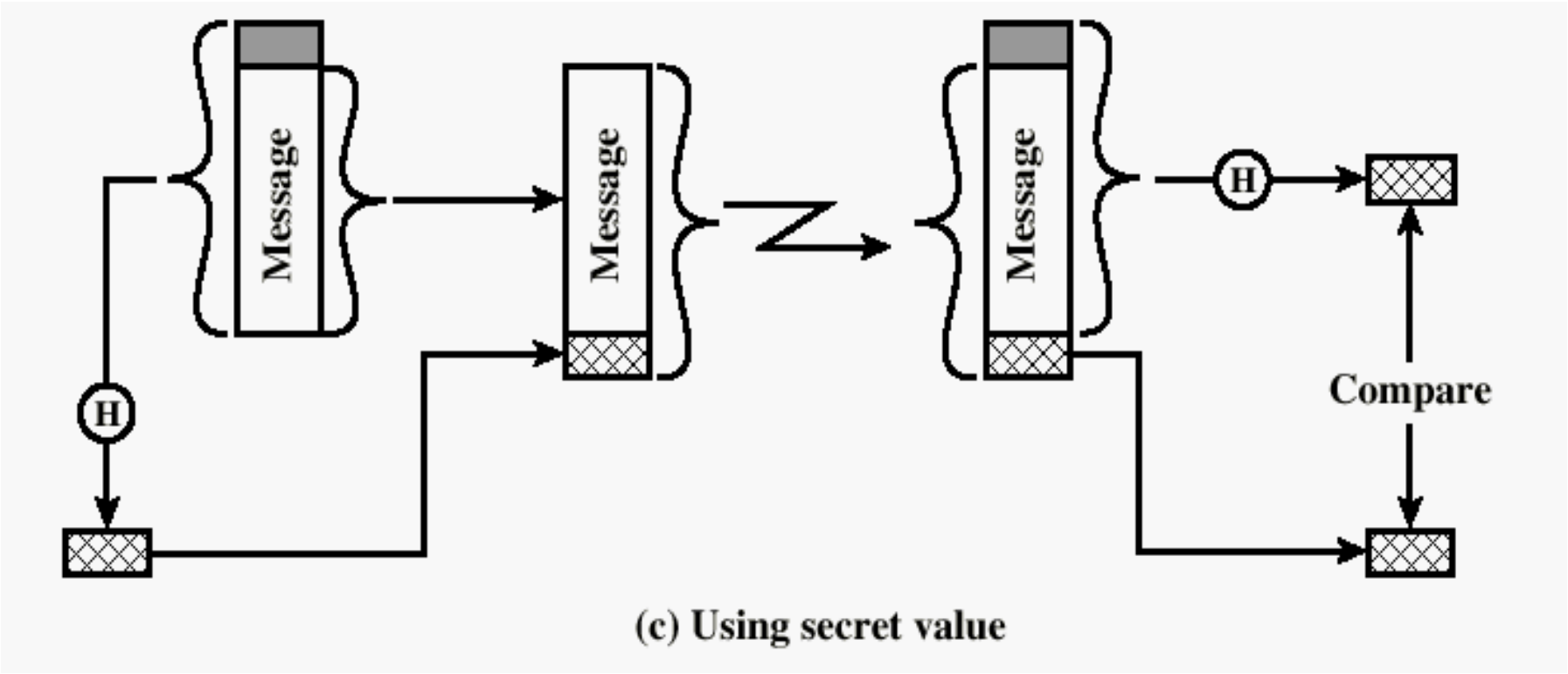
Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

One-way HASH function



One-way HASH function

- Secret value is added before the hash and removed before transmission.



(c) Using secret value

MD2

- **It takes a message of arbitrary length and produces 128-bit message digest.**
- ***Padding:***

- The message must be multiple of 16 octets.
  If the message is already multiple of 16 octets, 16 octets of padding are added,
  otherwise r octets (1<= r <=15) are added.
  Each pad octet contains the value r.
  Note that there must always be padding.
- **Example:**
  consider a message m = "abcdefghij" of 10 bytes,
  the value of r is 6 and the message is padded as follows: "abcdefghij666666".
- ***Checksum: Figure 5-4***
- A 16-byte checksum is appended to the message before computing the MD.

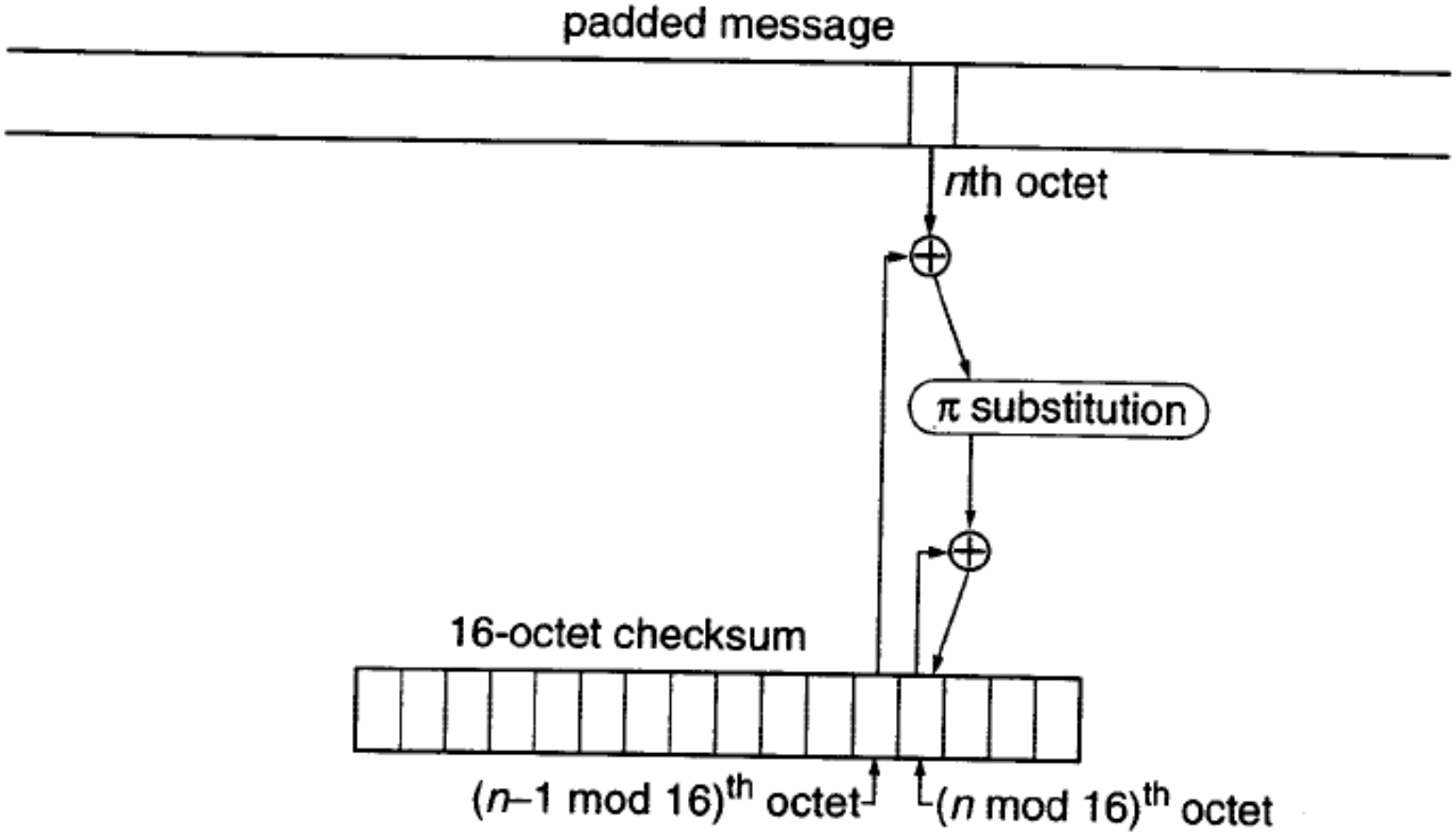


Figure 5-4. MD2 Checksum Calculation

41	46	67	201	162	216	124	1	61	54	84	161	236	240	6	19
98	167	5	243	192	199	115	140	152	147	43	217	188	76	130	202
30	155	87	60	253	212	224	22	103	66	111	24	138	23	229	18
190	78	196	214	218	158	222	73	160	251	245	142	187	47	238	122
169	104	121	145	21	178	7	63	148	194	16	137	11	34	95	33
128	127	93	154	90	144	50	39	53	62	204	231	191	247	151	3
255	25	48	179	72	165	181	209	215	94	146	42	172	86	170	198
79	184	56	210	150	164	125	182	118	252	107	226	156	116	4	241
69	157	112	89	100	113	135	32	134	91	207	101	230	45	168	2
27	96	37	173	174	176	185	246	28	70	97	105	52	64	126	15
85	71	163	35	221	81	175	58	195	92	249	206	186	197	234	38
44	83	13	110	133	40	132	9	211	223	205	244	65	129	77	82
106	220	55	200	108	193	171	250	36	225	123	8	12	189	177	74
120	136	149	139	227	99	232	109	233	203	213	254	59	0	29	57
242	239	183	14	102	88	208	228	166	119	114	248	235	117	75	10
49	68	80	180	143	237	31	26	219	153	141	51	159	17	131	20

Figure 5-5. MD2 π Substitution Table

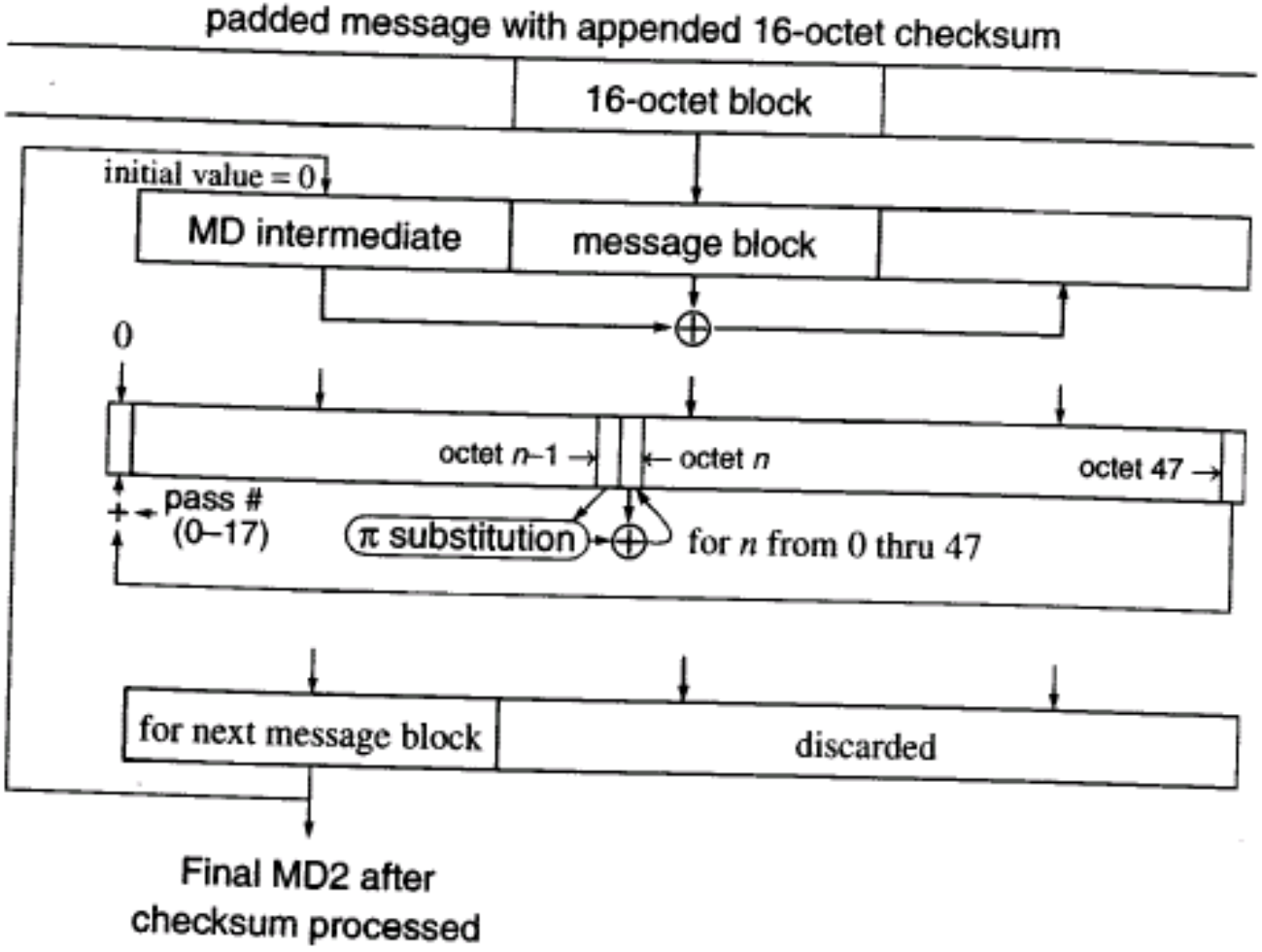


Figure 5-6. MD2 Final Pass

MD4

- **Was designed to be a 32-bit word oriented so it can be computed faster on 32-bit CPUs** rather **than an octet-oriented MD2.**

MD5

- **Was designed to be more concerned with security than speed.**
- ***All the MD family algorithms produce 128-bit digests.***

SHA-1

- **Designed by NIST to produce 160-bit digests (it is more secure than MD5 but little slower).**

HTTP Secure

Hypertext Transfer Protocol Secure (**HTTPS**) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems.

- The **Hypertext Transfer Protocol** (**HTTP**) is an Application Layer protocol for distributed, collaborative, hypermedia information systems. HTTP is a request/response standard typical of client-server computing. In HTTP, web browsers typically act as clients, while an application running on the computer hosting the web site acts as a server. The client, which submits HTTP requests, is also referred to as the *user agent*. The responding server, which stores or creates *resources* such as HTML files and images, may be called the *origin server*.

- SSL (***S**ecure **S**ockets **L**ayer)* a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with *https:* instead of *http*:.

- **Transport Layer Security** (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.
- TLS is an IETF standards track protocol

- The TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography. TLS provides RSA security with 1024 and 2048 bit strengths.