USING DATATYPE-PRESERVING ENCRYPTION TO ENHANCE DATA WAREHOUSE SECURITY

Harry E. Smith
Quest Database Consulting, Inc.
303-771-2246
hsmith@qdbc.com

Michael O. Brightwell
FM Software, Inc.
303-298-8262
mbrightw@fmsoftware.com

DATA WAREHOUSE VULNERABILITIES

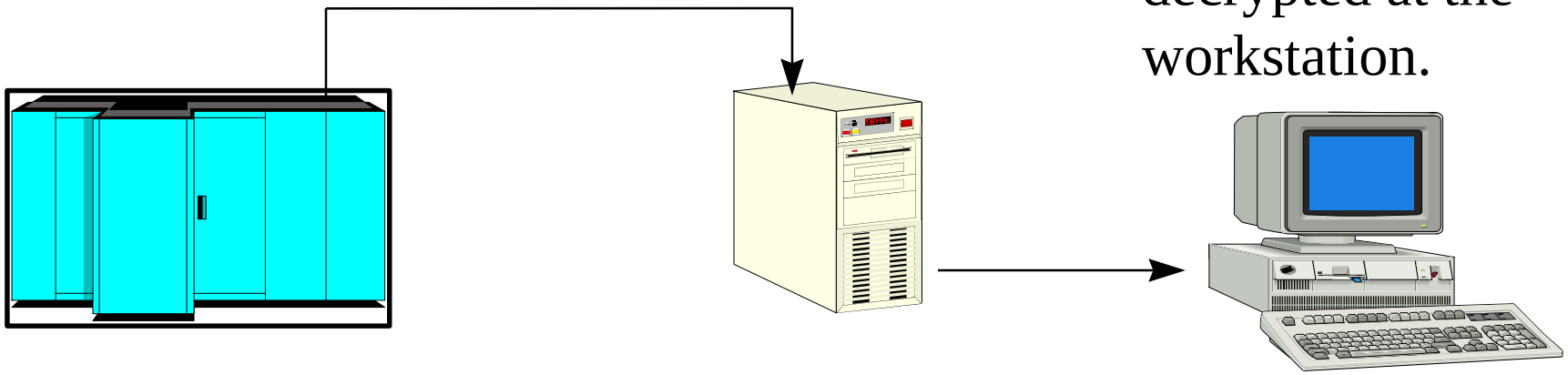
- Heterogeneous Environment
- Multiple Copies of Sensitive Data
- Deadline Pressure
- Concentrated Valuable Information
- Transmission Over Insecure Lines
- Unprotected Load Files
- Frequent Source and Target Changes

CRYPTOGRAPHIC APPROACH TO DATA WAREHOUSE SECURITY

1. Data is encrypted during the extraction process.

2. Intermediate files, load files and backups remain encrypted.

3. Data is decrypted at the workstation.



REQUIREMENTS

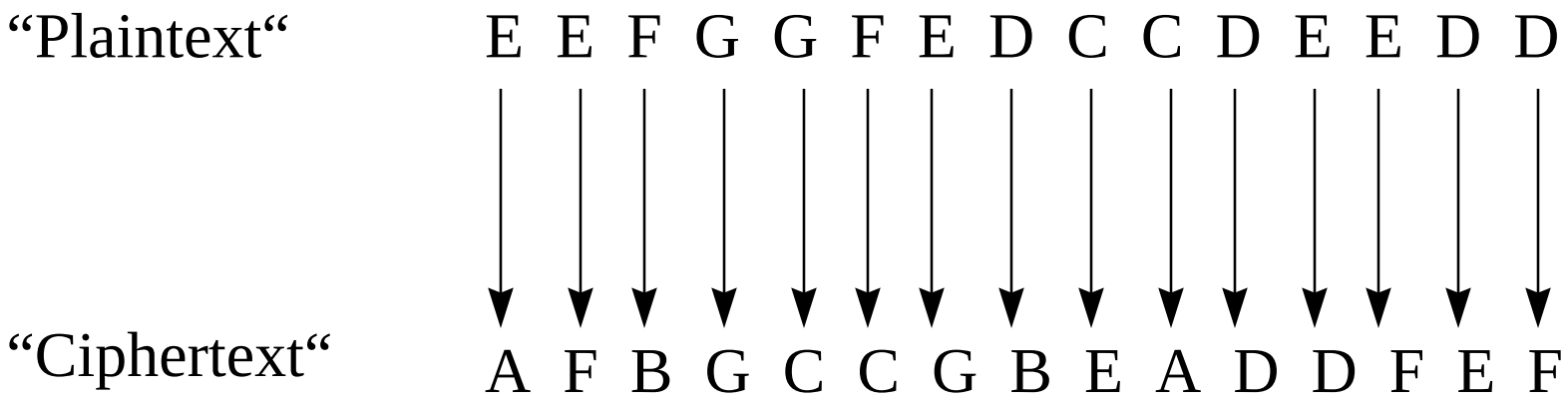
- Cryptographically Strong
- Work With Any DBMS and OS
- Work With Different Character Sets
- No Application or Database Changes
- No Programming Language Dependence
- Fail Safe

DATATYPE PRESERVATION

- Requires no DBA intervention.
- Loader Functions Normally
- Queries Function Normally*

* Important exception noted later.

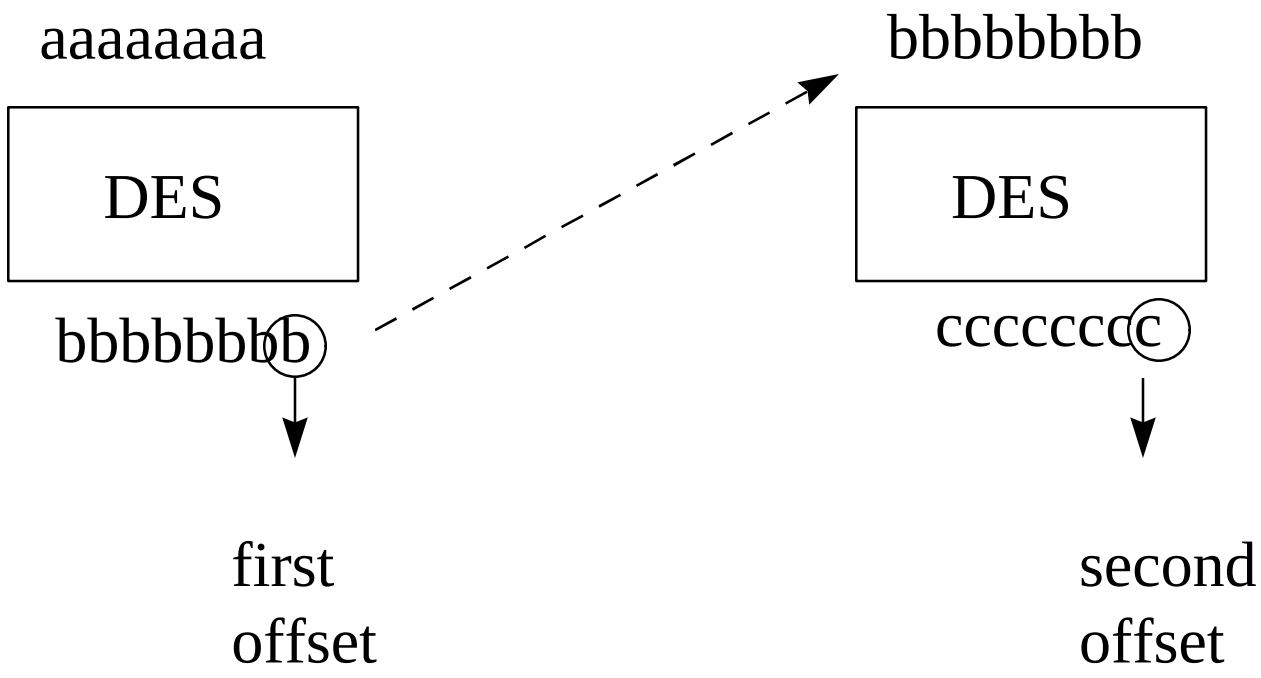
DATATYPE PRESERVATION EXAMPLE



DATATYPE PRESERVATION METHODOLOGY

“Alphabet“	A	B	C	D	E	F	G								
“Index Values“	0	1	2	3	4	5	6								
“Plaintext“	E	E	F	G	G	F	E	D	C	C	D	E	E	D	D
“Plaintext Indices“	4	4	5	6	6	5	4	3	2	2	3	4	4	3	3
“Encryption Offsets“	3	1	3	0	3	4	2	5	5	5	0	6	1	1	2
“Modular Sums“	0	5	1	6	2	2	6	1	4	0	3	3	5	4	5
“Ciphertext“	A	F	B	G	C	C	G	B	E	A	D	D	F	E	F

ENCRYPTION STRENGTH



USAGE CONSTRAINTS

- Encrypted Data May Be Misinterpreted
- Column Functions (SUM, AVG, MIN, MAX) May Not Be Used
- Key Distribution Problem Still Exists
- Key Compromise Requires Re-Encryption of Entire Database

ADDITIONAL APPLICATIONS

- Blind Keys
- Check Characters
- Software License Control

BREAK IT IF YOU CAN!