Cryptography

Caesar cipher

- Replace each letter in the plaintext with a letter found at a fixed shift down the alphabet
- For example, with a shift of 3:
  - D → A
  - E → B

Uryyb Jbeyq!

Vignère Cipher

- Use a different shift for each character position
- A *key* encodes the shift for each position
- Each character in the key is the shift from A for the matching position
  - Key "BEER" means that the first position is shifted by one, the second and third by 4 and the fourth by 17
- The key repeats to cover the whole message

Vignère Cipher - example

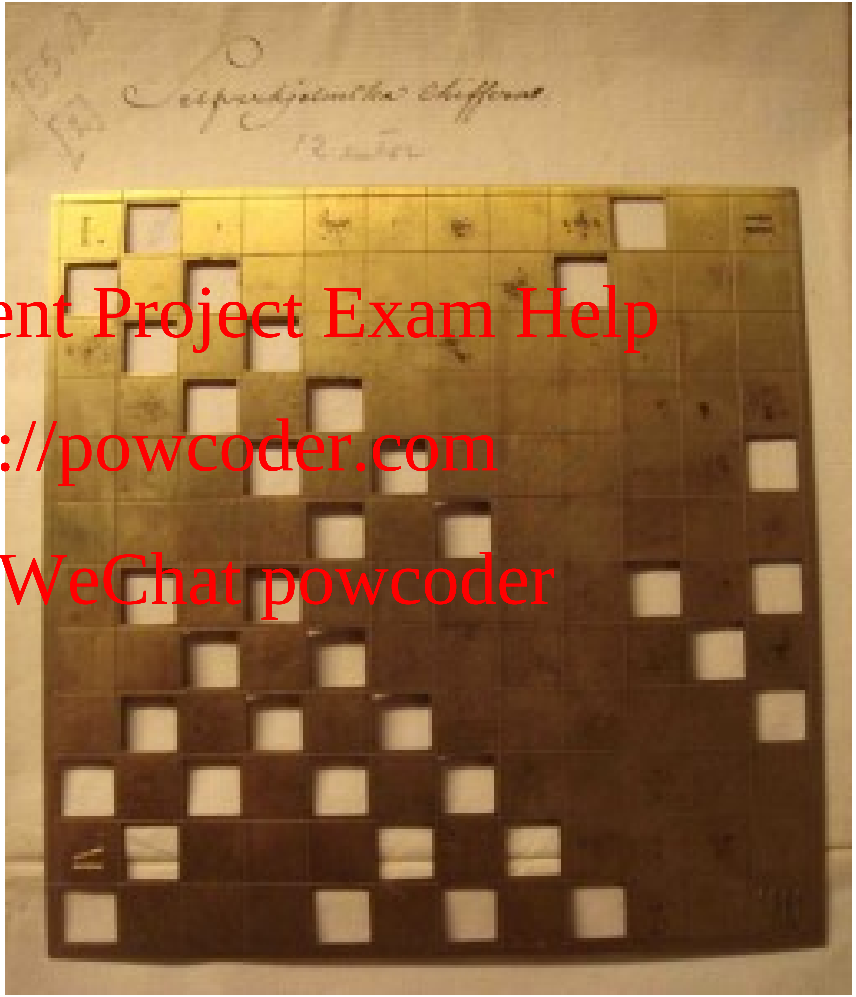
BEERB EERBE

Hello World!

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Scytale

Feissner Grille



How not to select a cipher?

- Kerckhoffs's principle
  - Don't use a secret scheme – rely only on the secrecy of the key

- Schneier's law

  - "**Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break**."

- The Dunning-Kruger effect

Proving Cipher Security

- A "formal definition"
- A cipher defined over $(\mathcal{K}, \mathcal{M}, C)$ is a pair of *efficient* functions (E, D)

$$E: \mathcal{K}\times\mathcal{M}\rightarrow C, \quad D: \mathcal{K}\times C\rightarrow\mathcal{M}$$

(We usually write $E_k(m)$ instead of $E(k,m)$)

For some definition of "efficient".

- Theoreticians use polynomial in the security parameter.
- We will think of it as fast enough to calculate

"Formal" definitions

- A cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ is a pair of *efficient* functions (E, D)

$$E: \mathcal{K}\times\mathcal{M}\rightarrow\mathcal{C}, \quad D: \mathcal{K}\times\mathcal{C}\rightarrow\mathcal{M}$$

(We usually write $E_k(m)$ instead of $E(k,m)$)

5pm at the rose garden?

$E_k()$

Gobbledy gobbledygook

Gobbledy gobbledygook

$D_k()$

5pm at the rose garden?

"Formal" definitions

- A cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ is a pair of *efficient* functions (E, D)

$$E: \mathcal{K}\times\mathcal{M}\rightarrow\mathcal{C}, \quad D: \mathcal{K}\times\mathcal{C}\rightarrow\mathcal{M}$$

(We usually write $E_k(m)$ instead of $E(k,m)$)

- Correctness:
  - $\forall m,k: D_k(E_k(m))=m$

Perfect Secrecy (Shannon 1945)

- An adversary that sees a ciphertext cannot learn anything about the plaintext.
  - All plaintexts have the same probability of producing any given ciphertext

- Formally:
  $\forall m_1, m_2, c: \Pr[E_k(m_1)=c] = \Pr[E_k(m_2)=c]$

- Questions:
  - Can we achieve perfect secrecy?
  - Does it guarantee security?

One Time Pad (Vernam 1919)

- Domain: $\mathcal{M}=\{0,1\}^n$, $\mathcal{C}=\{0,1\}^n$, $\mathcal{K}=\{0,1\}^n$
- For a plaintext m and a key k, $E_k(m)=k\oplus m$
- For a ciphertext c and a key k, $D_k(c)=k\oplus c$
  - Are these efficient?

- Correctness:
  - $D_k(E_k(m)) = D_k(k\oplus m) = k\oplus(k\oplus m) = (k\oplus k)\oplus m = 0\oplus m = m$

Perfect secrecy of OTP

- Recall: $\forall m_1, m_2, c$: $\Pr[E_k(m_1)=c] = \Pr[E_k(m_2)=c]$

- For every ciphertext c and plaintext m, there is exactly one key $k=c\oplus m$ such that $E_k(k,m)=c$

- Hence for all m and c, $\Pr[E_k(m)=c] = 2^{-n}$

- Because the probability of $E_k(m)=c$ does not depend on m, the cipher has perfect secrecy

Limitations

- Long key
  - Any perfectly secure cipher must have long keys
- Malleable
- Key cannot be used more than once
  - Class exercise: How would you break OTP if the key is used more than once?

- **Perfect secrecy assumes a very weak attacker!!!**

Ciphertext indistinguishability

- A desired property of ciphers

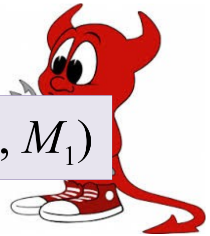
- A cipher is considered secure if no adversary can distinguish identify one of two messages based on their ciphertexts

- Typically presented as a game between an adversary and a challenger.

Distinguishability Games

k

$(E_k(m_b))$



(M_0, M_1)

- Challenger chooses a random key

- Adversary gets gets some access to a cipher with that key
- Adversary sends two messages to the challenger

- Challenger chooses one at random, encrypts it and sends back to adversary
- Adversary wins on a successful guess of the encrypted message

Adversarial models

- Known plaintext attack
  - The adversary learns some pairs of matching plaintexts and ciphertexts
- Chosen plaintext attacks
  - The adversary can encrypt some plaintexts of her choosing
- Chosen ciphertext attack
  - As CPA, but can also decrypt some ciphertexts
- Adaptive chosen ciphertext attack
  - AS CCA, but can base the choices on previous results

More attacks

- Side channel attacks
  - The adversary has information on the internal state of the implementation

- Fault injection attacks

  - The adversary can modify the internal state of the implementation

- Protocol attacks, RNG attacks, …

- **The adversary is not bounded!!!**

How to select a cipher?

- Use an established, well-researched encryption
  - E.g. AES, Salsa20
- Do not write a new implementation
  - Remember the Dunning-Kruger effect?
  - Use OpenSSL, libgcrypt, NaCl, etc.

Story time - CSS

- The DVD copy control association wanted to protect DVDs.
  - These are MGM, 20th Century Fox, Warner Bros etc.
  - They have a bit more resources than you, and likely more than your (future) employer
- 1996 – release CSS
  - Proprietary encryption algorithm
- Oct. 1999 – DeCSS appears. Presumably via reverse engineering a DVD drive.
  - Uses a 40-bit key. Not entirely CCA's fault, but could be broken in 24 hours using 1999's tech. (A few seconds today.)
- Nov. 1999 – Frank Stevenson releases three exploits
  - Reduce attack to 2^{25}. Can be broken in a few seconds.

Types of ciphers

- Stream ciphers
  - Produce a pseudo-random stream of bits
  - XOR stream of bits with plaintext message to produce ciphertext
- Block ciphers
  - Operate on fixed-size blocks of data
    - SWEET32 attack – ciphers with 64-bit blocks are not secure. Use AES (128-bit blocks).

- Block ciphers are better understood and are used more often

Substitution-Permutation Network

- An approach for designing block ciphers
- Consists of multiple rounds. Each round consists of two layers:
  - Substitution boxes – a bijective function of a small number of bits
  - Permutation box – a function that transposes bits from the input to the output

SP-Network

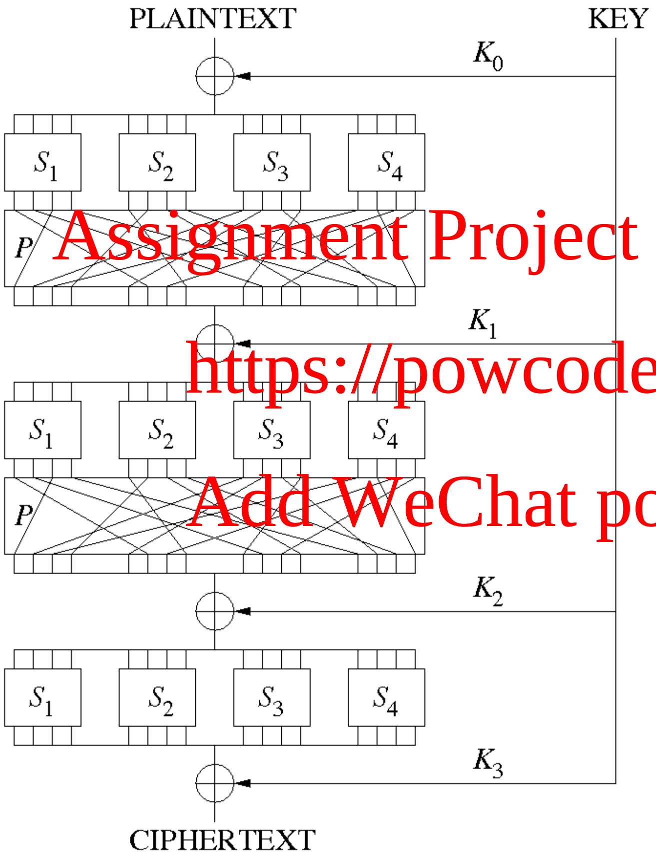
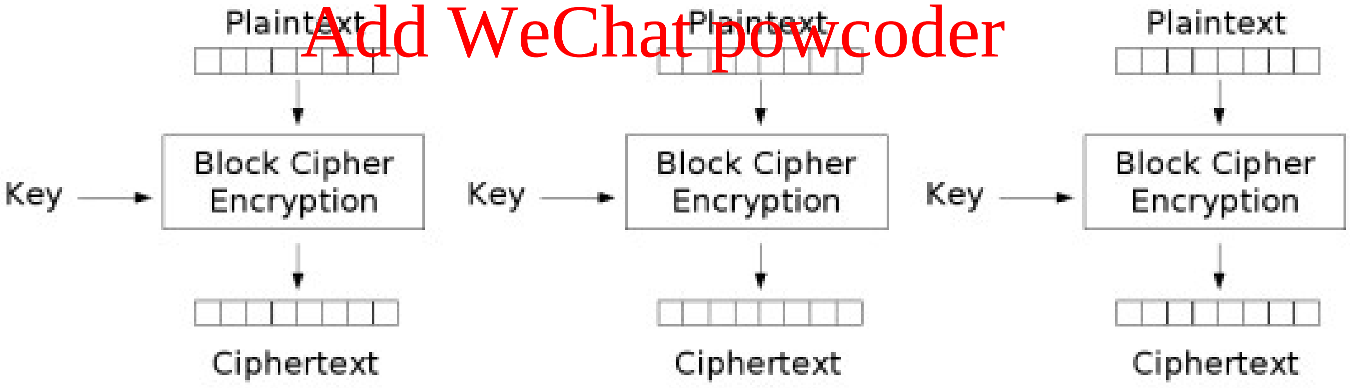


Diagram by Wikipedia user GaborPete

Modes of Operation – ECB

- The block cipher mode of operation specifies how to handle messages longer than a single block.
- Electronic codebook (ECB)
  - Divide message into blocks
  - Encrypt each block

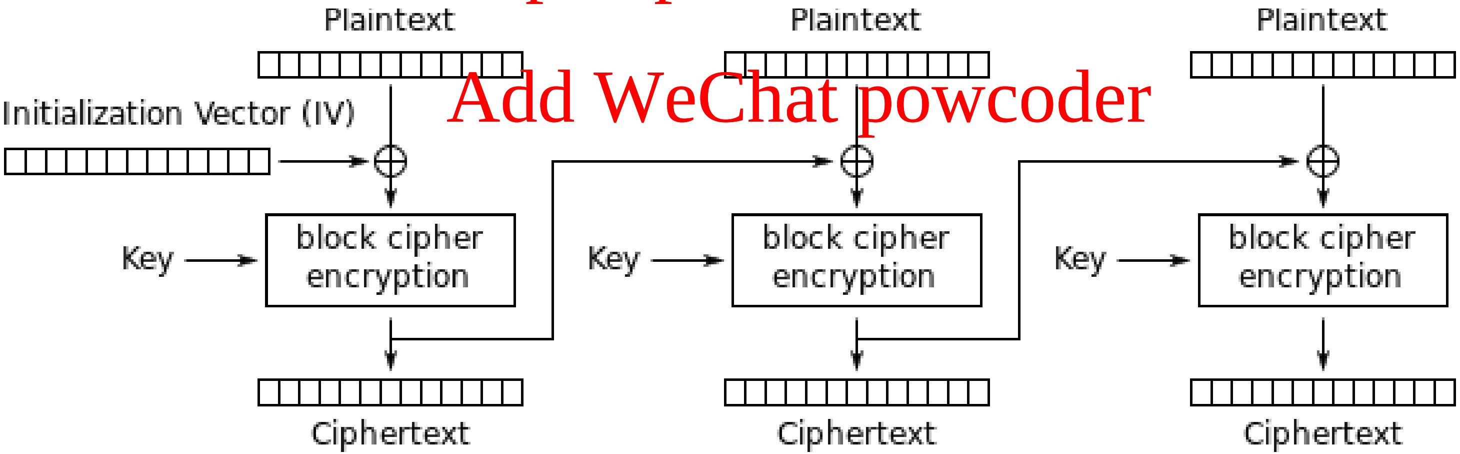


ECB is bad

- Identical plaintexts encrypted to identical ciphertexts

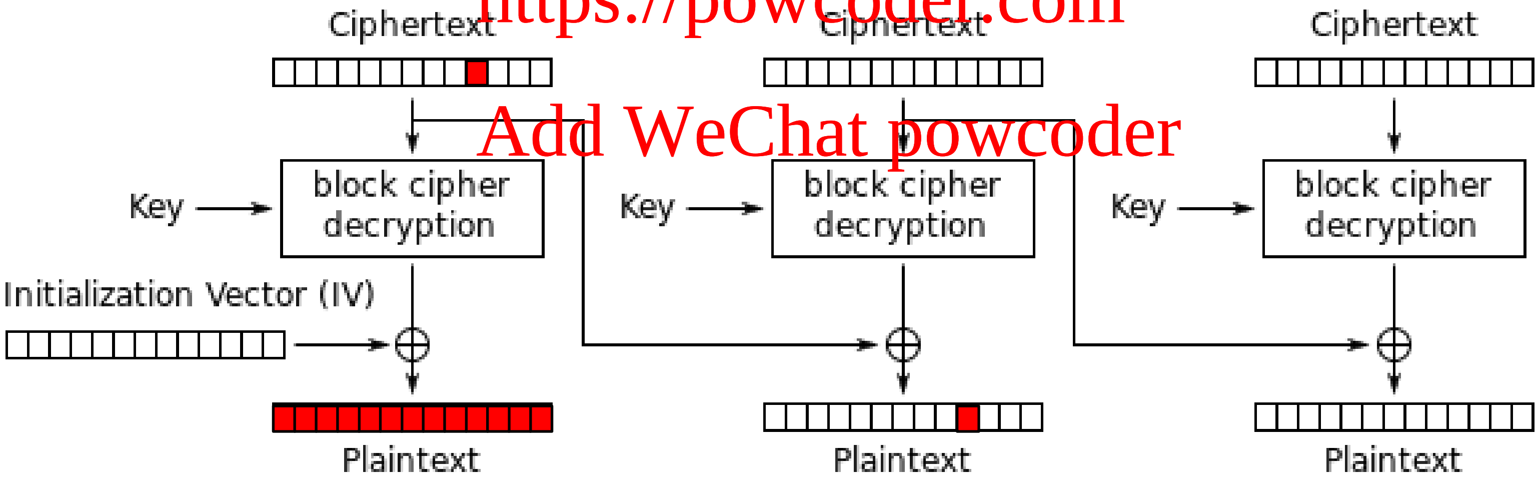
Modes of operation - CBC

- Cipher Block Chaining
  - Before encryption XOR each plaintext block with the previous ciphertext block
  - Use a random Initialisation Vector (IV) for the first block
    - IV does not need to remain secret



CBC Drawbacks

- Encryption (decryption) is sequential
- Limited ciphertext error propagation
  - Exploited in the POODLE and Lucky 13 attacks



Modes of operation - CTR

- Turns a block cipher into a stream cipher
  - Generate a sequence of “counter” blocks
    - Typically, a random nonce combined with a sequence number
  - Encrypt each counter block
  - XOR with the corresponding plaintext (ciphertext) block
- Supports parallel encryption (decryption)

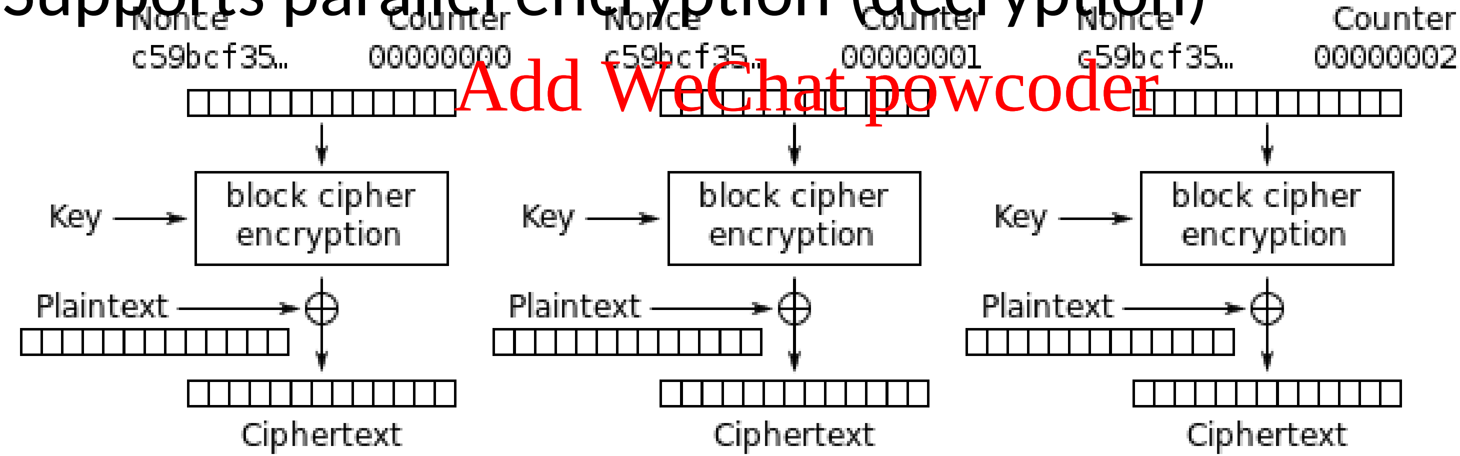


Diagram from Wikipedia

CTR - Drawbacks

- Malleable – a change in the ciphertext results causes a similar change in the plaintext
- Sensitive to repeated nonces and to an attacker manipulating the nonces

Modes of operation - Summary

- ECB – not secure. Do not use unless you know what you are doing.
  - Remember the Dunning-Kruger effect

- CBC – most commonly used.

- CTR – better performance but more sensitive

- No authentication
- No message integrity