Malleability continued, integrity

**Idea:** Given $Enc(k,m)$ for unknown $m$
adversary can produce another ciphertext
that decrypts to $m'$ that is "related" to $m$
(in a predictable way)

**Demo:**

base 64 encoding

3 raw data bytes $\rightarrow$ 4 printable characters

*In Javascript:*

```
$\begin{align*}
&\text{btoa} \\
&\text{atob}
\end{align*}$
```

"Ascii to Binary"

"Binary to Ascii"

*In Linux:*

```
$\text{echo "base64 encoded stuff" | base64 -d | xxd}$
```

**ECB mode:**

change 1 byte in ciphertext

$\Rightarrow$ entire block of plaintext changed

other blocks unchanged

remove block of ciphertext $\Rightarrow$ that block disappears from plaintext

rearrange / duplicate blocks ....
Change 1 byte of ciphertext ⇒ only that byte of plaintext changes
(except if 1 change IV ⇒ totally different plaintext)

CBC:
Dec Mode:
change 1 byte ⇒ clobbers 1 block completely & flips 1 byte in following block

XML encryption:
W3C standard for XML encryption, uses CBC

Attack scenario:
- Server receive CBC-encrypted XML command
- Decrypts ciphertext
- Gives an error if not well formatted
- Else executes command quietly
Attack: given $C$ containing unknown $m$ construct lots of related ciphertexts send to server, use responses to recover $m$ in entirety!