🔐 Demo: Azure Storage Encryption in Azure Portal

🔸 Goal: Show how **encryption at rest** works in Azure Storage and how to **configure customer-managed keys (CMK)** instead of Microsoft-managed ones.

✅ Part 1: Understanding Azure Storage Encryption

Quick Concepts (Slide or verbal):

- Azure automatically **encrypts all data at rest** in storage accounts.
- **Default**: Uses **Microsoft-managed keys**.
- You can switch to **Customer-managed keys (CMK)** stored in **Azure Key Vault** for more control.

🧪 Part 2: Hands-On Demo Steps (Azure Portal)

🛠️ Step 1: Create a New Storage Account

1. Go to **Azure Portal** → **Storage Accounts**
2. Click **"+ Create"**
3. Fill in:
   - **Subscription & Resource Group**
   - **Storage Account Name**
   - **Region** (e.g., East US)
   - **Performance**: Standard
   - **Redundancy**: LRS (or any)
4. **Important**: Under **Advanced** → Encryption:

- Leave it as **Microsoft-managed keys** for now.
- Click **Review + Create** → then **Create**

🔍 Step 2: View Default Encryption Settings

Once deployed:

1. Go to your Storage Account → **Settings** → **Encryption**
2. You'll see:
   - Encryption at rest ✅ enabled
   - **Microsoft-managed key** is being used

🗣️ *Say*: "By default, Microsoft handles the keys, so you don't have to. But if you want more control—like key rotation policies—you can use your own."

🗝️ Step 3: Use Customer-Managed Keys (CMK)

A. Create a Key Vault

1. Go to **Key Vaults** → **+ Create**
2. Fill in:
   - Name, Resource Group, Region
3. Click **Review + Create** → then **Create**

B. Add an Encryption Key to the Vault

1. Go to your new Key Vault
2. Click **Keys** → **+ Generate/Import**
3. Choose:

- Method: Generate
- Name: `storageKey1`
- Key Type: RSA

4. Click **Create**

C. Assign Access to Storage Account

1. In the **Key Vault**, go to **Access Configuration**
2. Ensure that **RBAC** is enabled for key permissions
3. Go to **Access control (IAM)** → **+ Add role assignment**
    - Role: **Key Vault Crypto Service Encryption User**
    - Assign to: Your storage account's identity (if system-assigned identity isn't enabled, enable it first)

D. Update Storage Account to Use CMK

1. Go back to your **Storage Account** → **Encryption**
2. Select: **Customer-managed key**
3. Choose:
    - **Key Vault URI**
    - Select the key you created (`storageKey1`)
4. Save changes

✅ Final Step: Confirm It’s Working

- Back in **Encryption settings**, it will now show **Customer-managed key** with Key Vault info.
- You can rotate keys manually in Key Vault or use automation.

🎯 Teaching Notes

Teaching Tip	Why it Helps
Use a real Azure subscription or sandbox (e.g. https://learn.microsoft.com/en-us/training/azure/)	Learners can follow along
Explain scenarios (e.g. finance apps needing CMK)	Connects concept to real use
Show both Microsoft-managed and CMK	Contrast helps retention
