Quick review

AES

- Secure, efficient symmetric encryption for data/messages
- Requires both parties to have same shared, private key

RSA

- Public key encryption whose security depends upon difficulty of factoring very large numbers
- Use for encrypting data/messages, key exchange, and digital signatures

Diffie-Hellman Key Exchange

- Public key whose security depends on DLP
- Only used for key exchange, not data/message encryption
- Both parties contribute to private key

Comparing Security Levels

Table 6.1 Bit lengths of public-key algorithms for different security levels

Algorithm Family	Cryptosystems	Security Level (bits)			
		(80)	128	192	256
Integer factorization	RSA	(1024 bits)	3072 bits	7680 bits	15360 bits
Discrete logarithm	DH, DSA, Elgamal	(1024 bits)	3072 bits	7680 bits	15360 bits
Elliptic curves	ECDH, ECDSA	(160 bits)	256 bits	384 bits	512 bits
Symmetric-key	e.g., AES	(80 bits)	128 bits	192 bits	256 bits

From Paar, Pelzl, and Güneysu, pg. 186

Some desirable properties of a cryptographic system

- **Confidentiality:** Information is kept secret from all but authorized parties
- **Integrity:** Messages have not been modified in transit
- **Message Authentication:** The sender of the message is authentic
- **Nonrepudiation:** The sender cannot deny the creation of the message

Digital Signature Algorithm, 160-bit

Key creation - Alice

- Find 1024-bit prime p,
  160-bit prime q where q divides $p - 1$
- Find $\alpha \in \mathbb{Z}_p^*$ where ord$(\alpha) = q$
- Choose private d where $0 < d < q$
  Compute $\beta \equiv \alpha^d \mod p$
- Publish (p, q, α, β)

Sign message x - Alice

- Choose ephemeral k_E where $0 < k_E < q$
- Compute
  $$r \equiv \left(\alpha^{k_E} \mod p\right) \mod q$$
  $$s \equiv \left(\text{SHA}(x) + dr\right) k_E^{-1} \mod q$$
- Send $(x, (r, s))$

Verify signature - Bob

- Compute
  $$w \equiv s^{-1} \mod q$$
  $$u_1 \equiv w \cdot \text{SHA}(x) \mod q$$
  $$u_2 \equiv w \cdot r \mod q$$
  $$v \equiv \left(\alpha^{u_1}\beta^{u_2} \mod p\right) \mod q$$
- If $v = r$ then valid
  If $v \neq r$ then invalid

Use Hash[x,"SHA3-256"] for the hash function in our small DSA

1. Alice publishes $(p, q, \alpha, \beta) = (241\,553\,623, 13\,033, 52\,824, 238\,101\,207)$
   (a) Verify that p, q and α are reasonable choices for our small version of DSA.

   (b) Which, if any, of the following are valid DSA signatures?
      (i) $(x,\ (r,s)) =$ ("Argybargy", $(5105, 11\,671)$)

      (ii) $(x,\ (r,s)) =$ ("Pleased to Meet Me", $(9543, 3174)$)

2. You want to use our small version of DSA to sign the message

   "My cabbages!"

   using values of $p = 2\,738\,078\,869$, $q = 65\,323$, and $\alpha = 11\,208$

   (a) Verify that p, q and α are reasonable choices for our small DSA.

   (b) Use $d = 17\,132$ to compute your value for β.

   (c) Use a value of $k_E = 41\,821$ to sign your message.