Algorithm RC4(byte string K)
byte i, j  // all arith involving these mod 256
for i ← 0 to 255 do S[i] ← i
j ← 0
for i ← 0 to 255 do
  j ← j + S[i] + K[i mod |K|]
  S[i] ↔ S[j]

i, j ← 0
repeat
  i ← i + 1
  j ← j + S[i]
  S[i] ↔ S[j]
output S[(S[i] + S[j]) mod 256]

RC4: BYTE^k → BYTE^∞
for any k ∈ [1..256]
Algorithm ChaCha20(key, ctr, non)

\[4\]

\[\text{state} \leftarrow \text{con} \mid \text{key} \mid \text{ctr} \mid \text{non}\]

\[s \leftarrow \text{state}\]

\[\text{for } i \leftarrow 1 \text{ to } 10 \text{ do}\]

\[\text{QR}(s[0], s[4], s[8], s[12]) \quad \text{// col 1}\]

\[\text{QR}(s[1], s[5], s[9], s[13]) \quad \text{// col 2}\]

\[\text{QR}(s[2], s[6], s[10], s[14]) \quad \text{// col 3}\]

\[\text{QR}(s[3], s[7], s[11], s[15]) \quad \text{// col 4}\]

\[\text{QR}(s[0], s[5], s[10], s[15]) \quad \text{// diag 1}\]

\[\text{QR}(s[1], s[6], s[11], s[12]) \quad \text{// diag 2}\]

\[\text{QR}(s[2], s[7], s[8], s[13]) \quad \text{// diag 3}\]

\[\text{QR}(s[3], s[4], s[9], s[14]) \quad \text{// diag 4}\]

\[\text{od}\]

\[\text{state} +\Rightarrow s\]

\[\text{return } \text{state}\]

---

ChaCha20
Dan Bernstein
2008

Algorithm QR(a, b, c, d)

\[a +\Rightarrow b; \quad d \leftarrow a; \quad d \ll 16;\]

\[c +\Rightarrow d; \quad b \leftarrow c; \quad b \ll 12;\]

\[a +\Rightarrow b; \quad d \leftarrow a; \quad d \ll 8;\]

\[c +\Rightarrow d; \quad b \leftarrow c; \quad b \ll 7;\]
ChaCha20
Nice design

1. Good choice of signature – PRF with 32, 16, 64 byte key, input, output
2. Security has held up very well – no remotely damaging attacks
3. Very fast in SW, with no special HW instructions (eg., 2.3 cpb Sandy Bridge)
4. Spare use of operations – “ARX” (add-rotate-xor are only ops used)
5. Constant time – no tables
6. Open design, no intelligence-agency involvement

7. No key-setup, no subkeys
DES

IBM/NSA
1975

DES: $\{0,1\}^{56} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$
Half Block (32 bits)  Subkey (48 bits)

E

\[
\begin{array}{cccccccc}
S1 & S2 & S3 & S4 & S5 & S6 & S7 & S8 \\
\end{array}
\]

P
# Definition of DES S-Boxes

<table>
<thead>
<tr>
<th>Row</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>Box</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>14</td>
<td>4</td>
<td>13</td>
<td>1</td>
<td>2</td>
<td>15</td>
<td>11</td>
<td>8</td>
<td>3</td>
<td>10</td>
<td>6</td>
<td>12</td>
<td>5</td>
<td>9</td>
<td>0</td>
<td>7</td>
<td>S1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>15</td>
<td>7</td>
<td>4</td>
<td>14</td>
<td>2</td>
<td>13</td>
<td>1</td>
<td>10</td>
<td>6</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>5</td>
<td>3</td>
<td>8</td>
<td>S2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>14</td>
<td>8</td>
<td>13</td>
<td>6</td>
<td>2</td>
<td>11</td>
<td>15</td>
<td>12</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>10</td>
<td>5</td>
<td>0</td>
<td>S3</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>12</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>7</td>
<td>5</td>
<td>11</td>
<td>3</td>
<td>14</td>
<td>10</td>
<td>0</td>
<td>6</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>15</td>
<td>1</td>
<td>8</td>
<td>14</td>
<td>6</td>
<td>11</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>7</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>0</td>
<td>5</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>13</td>
<td>4</td>
<td>7</td>
<td>15</td>
<td>2</td>
<td>8</td>
<td>14</td>
<td>12</td>
<td>0</td>
<td>1</td>
<td>10</td>
<td>6</td>
<td>9</td>
<td>11</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>14</td>
<td>7</td>
<td>11</td>
<td>10</td>
<td>4</td>
<td>13</td>
<td>1</td>
<td>5</td>
<td>8</td>
<td>12</td>
<td>6</td>
<td>9</td>
<td>3</td>
<td>12</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>8</td>
<td>10</td>
<td>1</td>
<td>3</td>
<td>15</td>
<td>4</td>
<td>2</td>
<td>11</td>
<td>6</td>
<td>7</td>
<td>12</td>
<td>0</td>
<td>5</td>
<td>14</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>10</td>
<td>0</td>
<td>9</td>
<td>14</td>
<td>6</td>
<td>3</td>
<td>15</td>
<td>5</td>
<td>1</td>
<td>13</td>
<td>12</td>
<td>7</td>
<td>11</td>
<td>4</td>
<td>2</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>13</td>
<td>7</td>
<td>0</td>
<td>9</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>10</td>
<td>2</td>
<td>8</td>
<td>5</td>
<td>14</td>
<td>12</td>
<td>11</td>
<td>15</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>13</td>
<td>6</td>
<td>4</td>
<td>9</td>
<td>8</td>
<td>15</td>
<td>3</td>
<td>0</td>
<td>11</td>
<td>1</td>
<td>2</td>
<td>12</td>
<td>5</td>
<td>10</td>
<td>14</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>10</td>
<td>13</td>
<td>0</td>
<td>6</td>
<td>10</td>
<td>1</td>
<td>3</td>
<td>15</td>
<td>8</td>
<td>9</td>
<td>4</td>
<td>5</td>
<td>11</td>
<td>12</td>
<td>7</td>
<td>S4</td>
</tr>
<tr>
<td>0</td>
<td>7</td>
<td>13</td>
<td>14</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>9</td>
<td>10</td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>5</td>
<td>11</td>
<td>12</td>
<td>4</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>13</td>
<td>8</td>
<td>11</td>
<td>5</td>
<td>6</td>
<td>15</td>
<td>0</td>
<td>3</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>12</td>
<td>1</td>
<td>10</td>
<td>14</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>13</td>
<td>6</td>
<td>9</td>
<td>0</td>
<td>12</td>
<td>11</td>
<td>7</td>
<td>13</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>14</td>
<td>5</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>15</td>
<td>0</td>
<td>6</td>
<td>10</td>
<td>1</td>
<td>13</td>
<td>8</td>
<td>9</td>
<td>4</td>
<td>5</td>
<td>11</td>
<td>12</td>
<td>7</td>
<td>2</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>10</td>
<td>11</td>
<td>6</td>
<td>8</td>
<td>5</td>
<td>3</td>
<td>15</td>
<td>13</td>
<td>0</td>
<td>14</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>14</td>
<td>11</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>7</td>
<td>13</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>15</td>
<td>10</td>
<td>3</td>
<td>9</td>
<td>8</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>13</td>
<td>7</td>
<td>8</td>
<td>15</td>
<td>9</td>
<td>12</td>
<td>5</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>8</td>
<td>12</td>
<td>7</td>
<td>1</td>
<td>14</td>
<td>2</td>
<td>13</td>
<td>6</td>
<td>15</td>
<td>0</td>
<td>9</td>
<td>10</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>12</td>
<td>1</td>
<td>10</td>
<td>15</td>
<td>9</td>
<td>2</td>
<td>6</td>
<td>8</td>
<td>0</td>
<td>13</td>
<td>3</td>
<td>4</td>
<td>14</td>
<td>7</td>
<td>5</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>15</td>
<td>4</td>
<td>2</td>
<td>7</td>
<td>12</td>
<td>9</td>
<td>5</td>
<td>6</td>
<td>1</td>
<td>13</td>
<td>14</td>
<td>0</td>
<td>11</td>
<td>3</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>9</td>
<td>14</td>
<td>15</td>
<td>5</td>
<td>2</td>
<td>8</td>
<td>12</td>
<td>3</td>
<td>7</td>
<td>0</td>
<td>4</td>
<td>10</td>
<td>1</td>
<td>13</td>
<td>11</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>12</td>
<td>9</td>
<td>5</td>
<td>15</td>
<td>10</td>
<td>11</td>
<td>14</td>
<td>1</td>
<td>7</td>
<td>6</td>
<td>0</td>
<td>8</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td>11</td>
<td>2</td>
<td>14</td>
<td>15</td>
<td>0</td>
<td>8</td>
<td>13</td>
<td>3</td>
<td>12</td>
<td>9</td>
<td>7</td>
<td>5</td>
<td>10</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>13</td>
<td>0</td>
<td>11</td>
<td>7</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>10</td>
<td>14</td>
<td>3</td>
<td>5</td>
<td>12</td>
<td>2</td>
<td>15</td>
<td>8</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>4</td>
<td>11</td>
<td>13</td>
<td>12</td>
<td>3</td>
<td>7</td>
<td>14</td>
<td>10</td>
<td>15</td>
<td>6</td>
<td>8</td>
<td>0</td>
<td>5</td>
<td>9</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>11</td>
<td>13</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>10</td>
<td>7</td>
<td>9</td>
<td>5</td>
<td>0</td>
<td>15</td>
<td>14</td>
<td>2</td>
<td>3</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>13</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>6</td>
<td>15</td>
<td>11</td>
<td>1</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>14</td>
<td>5</td>
<td>0</td>
<td>12</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>15</td>
<td>13</td>
<td>8</td>
<td>10</td>
<td>3</td>
<td>7</td>
<td>4</td>
<td>12</td>
<td>5</td>
<td>6</td>
<td>11</td>
<td>0</td>
<td>14</td>
<td>9</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>11</td>
<td>4</td>
<td>1</td>
<td>9</td>
<td>12</td>
<td>14</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>10</td>
<td>13</td>
<td>15</td>
<td>3</td>
<td>5</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>14</td>
<td>7</td>
<td>4</td>
<td>10</td>
<td>8</td>
<td>13</td>
<td>15</td>
<td>12</td>
<td>9</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>6</td>
<td>11</td>
<td>S8</td>
</tr>
</tbody>
</table>
DES
- Historically important but outmoded design
- Politics by way of mathematics

1. Has held up well for its key length
2. But key length is was chosen to permit governmental breaks
3. Other political choices, too: hardware requirement, IP/FP, standardization obstructions
4. Secret, non-competitive process. Design criteria secret (although eventually disclosed by Don Coppersmith, after everything had been figured out)
5. Led to the advances in cryptanalysis, particularly differential and linear cryptanalysis
6. Led to advances in theory, starting with Luby-Rackoff result
AES Rijndael

Joan Daemen and Vincent Rijmen
1998/2002

DES: \( \{0,1\}^{56} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64} \)
AES
Another nice design

1. Good signature
2. Security has held up very well – no remotely damaging attacks
3. Hardware support has emerged on Intel and other platforms, making the algorithm extremely fast (like 0.625 cpb when usage mode permits parallelism)
4. Not great without hardware support
5. Relatively large state and under-considered key setup
6. Open design with minimal intelligence-agency involvement
Switching lemma:
For any adversary $A$ making at most $q$ queries,

$$\Pr[\pi \leftarrow \text{Perm}(n): A^{\pi(.)} \Rightarrow 1] - \Pr[\rho \leftarrow \text{Func}(n,n): A^{\rho(.)} \Rightarrow 1] \leq q^2 / 2^{n+1}$$

Oracle $E(X)$
- if $X \in \text{Dom}(f)$ then return $f(X)$
- $Y \leftarrow \{0,1\}^n$
- if $Y \in \text{Ran}(f)$ then $\text{bad} \leftarrow \text{true}$, $Y \leftarrow \{0,1\}^n \setminus \text{Ran}(f)$
- return $Y$

Fundamental lemma of game playing:
If games $G$ and $H$ are identical-until-$\text{bad}$, then

$$\text{Adv}_{G,H}^\text{dist} (A) = \Pr[A^G \Rightarrow 1] - \Pr[A^H \Rightarrow 1] \leq \Pr[G \text{ sets bad}].$$
CTR[$E$]

\[
\begin{align*}
\langle \text{Ctr},0 \rangle & \rightarrow E_K \\
\langle \text{Ctr},1 \rangle & \rightarrow E_K \\
\langle \text{Ctr},2 \rangle & \rightarrow E_K
\end{align*}
\]

\[\oplus\]

\[C\]

\[M\]
CTR[P]
CTR[$R$]
Theorem: Let $E$ be an $n$-bit blockcipher, let $\Pi=\text{CTR}[E]$, and let $A$ be an adversary (for breaking $\Pi$) that asks at most $\sigma$ blocks. Then there’s an adversary $B$ that gets advantage

$$\text{Adv}_{E}^\text{prp}(B) \geq 0.5 \text{Adv}_{\Pi}^\text{ind}(A) - \frac{\sigma^2}{2^{n+1}}$$

Adversary $B$ asks $\sigma$ queries and run in time approximately that of $A$. 
Define the prp-advantage $\text{Adv}_{E}^{\text{prp}}(A)$ of adversary $A$ attacking $E:\{0,1\}^{k} \times \{0,1\}^{n} \rightarrow \{0,1\}^{n}$ is the number

$$\Pr \left[ \text{Pr} \right]$$

Question #2

Not graded / anonymous on a separate piece of paper if you prefer:

How much do you think you understand of our class:

- Very little
- About half
- Most things
- Almost everything

Any suggestions for how I can do better?
What exciting event will happen Friday, Feb 8, in this very class?! 

Question #1

Why is it preferred for a PRF/PRP to run in constant time?

Question #2
Consider the PRG $G: \{0,1\}^{100} \rightarrow \{0,1\}^{200}$ defined by

$$G(x) = x \ || \ x$$

An adversary $A$ can do well in breaking $G$ by taking in a 200-bit string $y = y_1 \ y_2$ (where $|y_1| = |y_2|$) and answering 1 if

Question #1

and answering 0 otherwise.

This adversary gets advantage

Question #2